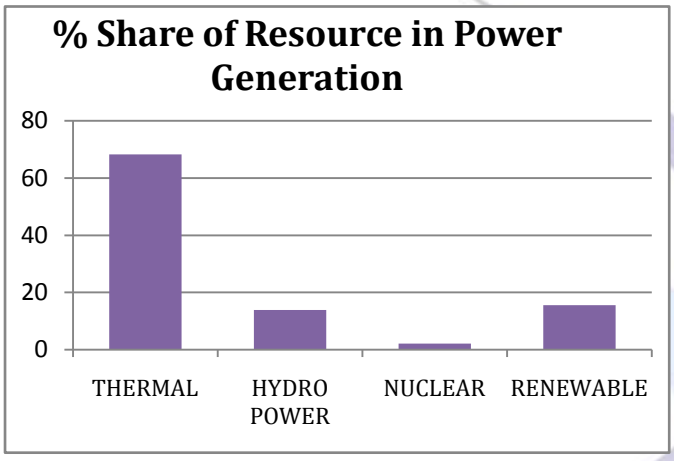
Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
40/17

CAN CHINA CAUSE POWER OUTAGE IN INDIA: OPERATION BLACKOUT?

Wg Cdr A Shrivastava
Research Fellow, CAPS

The electricity sector in India is growing at a rapid pace. During the year 2016-17, the Peak Demand was about 159 GW against the installed generation capacity of 319.6 GW. The share of generation capacity is as shown in the diagram below.



The natural resources for electricity generation in India are unevenly dispersed and concentrated in a few pockets. Hydro resources are located in the Himalayan foothills and the North Eastern Region. Coal reserves are concentrated in Jharkhand, Odisha, West Bengal, Chhattisgarh, Madhya Pradesh, Tamil Nadu and Gujarat. Therefore, an extensive network of transmission lines had to be developed crisscrossing the country for drawing power produced from different electricity generating stations and distributing the same to the consumers. This network of transmission lines is called the Power Grid and is controlled by large Industrial Control Systems (ICS). Unlike the traditional power grid, the modern 'smart' grids are designed to accommodate a two-way flow of both electricity and consumption (load) data. The new ICS are equipped with smart computing devices called SCADA[1] (Supervisory Control and Data Acquisition) systems which monitor the health of the networks.

The Times of India had, on January 21, 2017, first reported the vulnerability of India's transmission network to hacking in an 'intelligent' environment in which machines 'talk' to each other on a common platform. Indian power equipment manufacturers have repeatedly been raising alarm over the issue as power grids are being smartened up with SCADA.

While the command and control systems of plants and distribution networks were semi-isolated in the past, SCADA turns the entire power system into one giant network, raising not only efficiency but also vulnerability. The concerns being raised by Indian Electrical Equipment Manufacturers Association have largely come against a backdrop of smart grid contracts being dominated by Chinese firms. These firms have bagged SCADA contracts for more than 18 cities and many more are on the anvil. Besides, they have also qualified to bid for three transmission links being laid by the Centre to strengthen the national grid. SCADA contracts have long tenures which includes maintenance of equipment. Further, most transmission lines are given on BOT (Build, Operate, Transfer) basis where-in the contract period spans over 30 years. This permits the contractors to place their personnel (foreigners) on site and control/ monitor the operations in transmission lines. This arrangement may give ample scope to an adversary to plant potential bugs in the system which could be remotely activated at a later date just like the Stuxnet[2] virus attack and others.

How Secure is our Smart Grid?

The U.S. Department of Energy released a report in January 2017 which highlighted that the U.S. electric grid is in imminent danger from a cyber attack. In the department's Quadrennial Energy Review, it suggested that a widespread power outage can be caused by a cyber attack which could undermine 'critical defence infrastructure', cripple financial institutions and risk the health and safety of US citizens. The U.S. Department of Energy report highlighted that the next round of grid outages could be like the recent Shamoon malware[3] attack that hit Gulf State organizations, or the 'Black Energy'[4] attack in Ukraine. Today, the cyber world has changed dramatically; cyber-attacks on ICS/SCADA networks are more frequent and damaging. Therefore, investment in knowledge and awareness at the top levels of governance towards cyber security is an absolute priority for companies/ organisations/ governments.

Threats, risks and dangers related to cyber-security are changing

Experts warn that there is a possibility that ransomware developers will start targeting industrial control systems (ICS). The CRITIFENCE[5] security company and the team at the Georgia Institute of Technology created a Proof-of-Concept (PoC) ransomware, designed especially for ICS attacks, which relies on programmable logic controllers (PLCs). On April 26, 2017, at Security Week's 2017 Singapore ICS Cyber Security Conference, an ICS security consultant, Alexandru Ariciu, demonstrated ransomware attacks (which he called "Scythe") were able to target inconspicuous and less risky SCADA devices. The names of the targets are not revealed but he describes the affected devices as several types of I/O systems which stand

between OPC servers and field devices. The devices run a web server and are powered by an embedded operating system. He says that a large number of these systems are unprotected and easily accessible online, which allows crooks to hijack them by replacing their firmware with a malicious code.

In February 2015, Philippines National Grid ended technical co-operation with State Grid Corporation of China and expelled Chinese technicians over security concerns. In January 2016, U.S. investigators found proof that a cyber-attack can take down a power grid. In August 2016, Australia scuppered bids by State Grid Corporation of China and Hong Kong based Cheung Kong Infrastructure Holding Ltd for stakes in AustGrid over national security concerns. In October 2016, Germany withdrew approval for takeover of semiconductor supplier Aixtron SE by the local arm of China's Fujian Grand Chip Investment Fund. Power grid attacks could virtually paralyse a nation by causing disruption to services like railways, metro, water supply, communications, etc. It can also cripple the entire banking and financial services, disrupt medical and health facilities, challenge security setup, etc.

India's Concern

India is set to see a countrywide cyber security audit of its power distribution and generation system to prevent hacking as state grids and plants increasingly become smarter with large-scale deployment of digital technology. During May, 2017, at the State Energy Ministers' conference, piloted by the Union Power Minister, Piyush Goyal, all participants agreed to get their power system regularly audited by agencies empanelled by the Computer Emergency Response Team (CERT-In)[6]. The states also agreed to conduct mock drills simulating disasters and hackings to test preparedness for reviving downed systems. The concerns being raised by Indian Electrical Equipment Manufacturers Association have largely come against a backdrop of smart grid contracts being dominated by Chinese firms.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Notes

[1] SCADA is a computer based industrial automation control system that practically makes factories and utilities run on their own. In an electrical system, SCADA maintains balance between demand and supply in the grid.
[2] **Stuxnet** is a malicious computer worm, first identified in 2010, and was responsible for causing substantial damage to Iran's nuclear program. The software was designed to erase itself in 2012 thus limiting the scope of its effects.
[3] These attacks, which occurred in November 2016 and January 2017, reportedly affected thousands of computers across multiple government and civil organizations in Saudi Arabia and elsewhere in Gulf states. Shamoon was designed to destroy computer hard drives by wiping the master boot record (MBR) and data irretrievably.
[4] Dec 23, 2015, shut down over 30 sub-stations of power distribution system of Ukraine resulted in complete black out for 1-6 hrs in peak winters for over 2.3 lake people.
[5] CRITIFENCE is a Cyber Security solutions provider company for Critical Infrastructure, SCADA and Industrial Control Systems networks.
[6]CERT-In is the government's cyber warrior and has long experience of tackling hacking threats.