Is India prepared to protect its critical infrastructure assets from cyber threats?

By Rajabahadur V. Arcot,
Independent Industry Analyst / columnist and Automation Consultant with extensive experience in writing industry and technology trend articles, market research reports, case studies, white papers, and automation & manufacturing IT insights
rajabahadurav@gmail.com

Just think of series of incidents taking place in quick succession across the country that cripples power & water supplies and communication and transportation services to understand their debilitating effects on our lives. A cyber-attack can trigger all these and many more catastrophic incidents that will have grave consequences. This is not a preamble to a science fiction but a depiction of things happening in the cyberspace. While most of us are well aware of how information technology is transforming our lives in positive ways, many are not cognizant of its down side, the cyber vulnerabilities. Highly skilled and organized cyber attackers, which include nation states as well, have developed cyber weapons that target critical infrastructure assets. It is important for India, which is in the process of building critical infrastructure assets as part of its economic growth ambitions, to reckon with its geo-political compulsions, recognize the true nature of the threats, and develop strategies to secure their protection from cyberattacks.

The recent revelations of Edward Snowden and reports on Stuxnet, Duqu, Flame, Shamoon, Dragonfly and similar others provide us a glimpse of how cyberspace is emerging as the major battleground to gather intelligence and launch subversive activities. The cyber weapons are low-cost and yet very powerful that possess both offensive and defensive capabilities. They can effectively take down critical assets on which a country's national and economic security depends.

Cyber threat perceptions

The consequences of cyber-attacks are truly serious and that necessitated President Barak Obama to issue an executive order on this issue for improving the US Critical Infrastructure Cyber Security. The blog '"The Comprehensive National Cybersecurity Initiative" on www.whitehouse.gov says that the President has identified cybersecurity as one of the most serious economic and national security challenges that confronts the US. He adds that the government and the country are not adequately prepared to counter them. If what is widely written in numerous articles and reports are true, then the US was involved with Stuxnet, a malware that crippled the Iranian centrifuges; therefore, the US President knows best about

the true implications of cyber-attacks in their new manifestations. According to the recent poll conducted by Defense News Leadership and underwritten by United Technologies, almost half of US national security leaders who responded to the poll are of the opinion that cyber warfare as the most serious threat facing the United States. Israel's Major General Aviv Kochavi, speaking at the annual conference of the Institute for National Security Studies in Tel Aviv, said, "Cyber, in my modest opinion, will soon be revealed to be the biggest revolution in warfare, more than gunpowder and the utilization of air power in the last century." David Cameron, Briton's Prime Minister, writing in The Telegraph, has warned that the country faces changing threats in the form of global terrorism and unseen cyber criminals who can target the country from abroad and pledged £1.1 billion for defense to fight cyber terrorists.

Cyberattack targets control systems and critical infrastructure assets

Stuxnet, a computer malware that targeted industrial sites in Iran – a uranium enrichment plant - is a good example of a cyberattack on critical national assets. Stuxnet successfully destroyed the centrifuges by changing, without the knowledge of the uranium enrichment plant-operators, the set point at which the centrifuges are supposed to rotate. It is the first known reported case of a malware that explicitly and successfully attacked the industrial control systems. While it established the offensive capabilities of cyberattack, the most recent discovered malware dragonfly shows the information gathering activities in the cyberspace that could be a precursor to launch cyberattacks in future.

Security firms, Symantec and F-Secure, have recently released information about the malware Dragonfly / Havex RAT. According to Symantec, the targets of Dragonfly include energy grid operators, major electricity generation firms, and petroleum pipeline operators and it attacks industry industrial control systems. It uses the 'remote access Trojan' (RAT) and according to the reports available in the public domain, the malware uses websites of software companies including ICS suppliers to install malware versions of legitimate apps in targeted systems.

The Trojan communicates with a Command and Control (C&C) servers. It can drop and execute files without the user of control systems and their vendors being aware of this. By this, the attacker gains access and the means to control of the target systems. The target systems control the operations of critical infrastructure industries. The data-harvesting component, acting as an intelligence-collecting tool, gathers details about the operating systems, connected devices, such as the connected control system devices, network, vendor information, tag (identification) numbers, and similar others and sends them back to the command and control centers for further analysis of hackers. It also has credential-harvesting tool that gathers password details to aid further subversive actions. It is a sophisticated attack and only time would reveal the true implications of Dragonfly.

The ICS-CERT of the US reports of the infection of the software installers on at least three ICS vendor web sites. It further states that ICS-CERT testing has determined that the malware

payload has caused multiple common OPC platforms to intermittently crash. This could have a denial of service effect on applications that are reliant on OPC communications. The OPC acronym comes from "OLE (Object Linking and Embedding) for Process Control" and is a software interface standard.

With the information that the malware collects, the organization behind Dragonfly has all the necessary information to attack at will the critical infrastructure companies that it is interested in targeting. It has the tag numbers of the important regulated parameters, passwords necessary to change the set points, and details of the operating systems and hence their known vulnerabilities. With these operating details available, it would not be a big challenge for the cyber criminals to sabotage the operation of the targeted infrastructure companies engaged in producing electricity, distributing water supply, operating airports and rail transportation, providing communication services, and such others.

Is India doing enough?

Groups possessing high degree of cyber hacking skills, sophistication, and resources are involved in such activities. They include even state actors or other groups acting at their behest or on behalf of non-state actors. The canvas is so wide that it is even difficult to imagine the scope of the future cyber-attacks much less prepare an effective defense against them.

While all countries face cyber threats, India because of its geo-political compulsions is highly vulnerable. Except for the information that the Stuxnet malware has infected a large number of installations in India and that the government has authorized 'National Critical Information Infrastructure Protection Centre' (NCIIPC) to take all necessary measures to facilitate safe, secure, and resilient Information Infrastructure for Critical Sectors in the country no other information is available in the public domain. NCIIPC is under of National Technical Research Organization (NTRO). Additionally, the government of India's Inter Departmental Information Security Task Force (ISTF) has set up *Indian Computer Emergency Response Team* (CERT-In) to respond to the cyber security incidents and take steps to prevent recurrence of the same. Lack of credible information about the measures that NCIIPC is taking in protecting the country from cyber threats is a cause of concern. NCIIPC's charter mandates that it should "raise information security awareness among all stakeholders" and it is failing in its duty by its silence. While almost all leading *Computer Emergency Response Teams* (CERT) are regularly issuing alerts about the vulnerabilities, it is annoying to find that even the website of its Indian counterpart (CERT-In) is not accessible most of the time. In matters such as the cyber security threats to the country's critical infrastructure industry, it is critical to get all stakeholders on the same page and a certain degree of openness is absolutely necessary to create necessary awareness and ensure their commitment to take appropriate actions. More proactive measures such as organizing seminars and training workshops, involving the academia in starting appropriate courses, initiating a dialogue with the information technology companies and seeking their involvement in software testing are needed to prepare the country for future eventualities. Creating awareness among the critical infrastructure industries so that they are

future ready for such contingencies is critically important. In my humble opinion, self-reliance is the way forward while fully collaborating with all the global initiatives. Based on the success achieved in space and nuclear technologies thanks to domestic institutions such as Indian Space Research Organization and Bhabha Atomic Research Center, it is time for the policy makers to initiate appropriate measures.

About the Author

Rajabahadur V. Arcot is an Independent Industry Analyst / Columnist and Business Consultant with around 40 years of senior managerial experience. He has held C-level executive positions in leading companies, such as Honeywell, Thermax, Bells Controls an affiliate of Foxboro / Invensys, Electronics Corporation of India Limited and Instrumentation Limited. Until recently, he was responsible for ARC Advisory Group's business operations in India. He writes industry and technology trend articles, market research reports, case studies, white papers, and automation & manufacturing IT insights