Attacks on the Critical Infrastructure of Pakistan

Kaukab Jamal Zuberi
Cheif Editor

It was May 29, 2009, when the White House released the text of President Obama's speech on establishing a new cybersecurity office in White House. He mentioned "This world -- cyberspace -- is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives.

It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history.

So, cyberspace is real. And so are the risks that come with it."

In 2013, Snowden revealed that Pakistan, after Iran, was the most targeted country for surveillance by National Security Agency.

Microsoft also revealed that Pakistan witnessed the highest malware attack in mid of 2015. Later senate committee was shaped to bring a report on cyber threats and the committee revealed that Pakistan was among the top countries under foreign espionage. A country that is hostile to Pakistan is heavily attacking Pakistan. India has been hacking websites of the Pakistani government since 1998 with mostly denial-of-service (DoS). The reports show that between 1999 to 2008 nearly 1600 Pakistani websites were targeted by Indian hackers.

The websites of NAB, Education Ministry, NADRA, Ministry of Foreign Affairs, Finance Ministry and State Bank of Pakistan were hacked previously.

Prevention of Electronic Crime Act (PECA) came into force in 2016. Critical Infrastructure is defined under the act as follows:

"(x) "critical infrastructure" means critical elements of infrastructure namely assets, facilities, systems, networks or processes the loss or compromise of which could result in,

(a) major detrimental impact on the availability, integrity or delivery of essential services including those services, whose integrity, if compromised, could result in significant loss of life or casualties, taking into account significant economic or social impacts; or

(b) significant impact on national security, national defense, or the functioning of the state: Provided that the Government may designate any private or Government infrastructure in accordance with the objectives of sub¬paragraphs (i) and (ii) above, as critical infrastructure as may be prescribed under this Act;"

Section 6,7,8 of PECA defines the offences against the critical infrastructure, while section 10 link these offences to Cyber Terrorism as follows:

"10. Cyber terrorism: - Whoever commits or threatens to commit any of the offences under sections 6, 7, 8 or 9, where the commission or threat is with the intent to,—

(a) coerce, intimidate, create a sense of fear, panic, or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or

(b) advance inter¬faith, sectarian or ethnic hatred; or

(c) advance the objectives of organizations or individuals or groups proscribed under the law, shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both."

As per the definition of PECA, earlier cyber-attacks were the act of cyber terrorism and the attacks on the critical infrastructure after August 2016 were punishable as per the punishments defined under the Act.

In July 2021, Pakistan announced its long due National Cyber Security Policy. One of the guiding principles of the policy was that the government "Will regard a cyber-attack on Pakistan CI/ CII as an act of aggression against national sovereignty and will defend itself with appropriate response measures." The policy mentioned that every organization will be responsible for its cyber security and in case of a cyber-attack, the government will take lead the national response with help of the public and private sector.

However, this policy was announced without timelines and identifying the responsible organization to implement the national cybersecurity policy. The sense of urgency to safeguard our critical cyber infrastructure was missing from our National Cybersecurity policy.

August attacks on FBR infrastructure is a classic example of the poor handling of the incidents. The role of government agencies in determining those responsible for these attacks and ultimately punishing them is yet to be seen. In both the incidents, Microsoft Hyper V terminals were involved. Poor defense mechanism and sheer incompetence was revealed during this attack. The former Chief US diplomat for South Asian Affairs, Alice Wells, during her visit to Pakistan accused FBR of using a pirated version of Microsoft Hyper-V software and warned that FBR might become a target of cybercrime due to the use of a pirated software.

There are at least three versions of how hackers gained access to the critical infrastructure of FBR. The first version from technical wing of FBR stated that hackers gained accessed by using the vulnerabilities of Microsoft Hyper V terminals. The second version stated that the hackers disrupted the system by hacking the login ids and passwords of the data centre administrators and the third version, which was published in the report prepared by a local firm stated that the hackers used Spear-phishing emails as the medium for this breach. As a result of these lukewarm and complete the file type responses, HackRead, which is a news platform that centres on InfoSec, Cyber Crime, Privacy, Surveillance and hacking news reported that the confidential data of taxpayers was stolen in this breach. Furthermore, HackRead claimed that FBR's data was put on sale on a Russian Forum for $30,000.

This was an act of Cyber Terrorism, and the investigation lacked the vigor used to solve terrorism cases. The minister of technology announced on November 02, 2022, that millions of cyber attacks were being made in Pakistan every day.

Pakistan lacks a coordinated effort to combat the increasing threat on its critical infrastructure and critical information infrastructure. Immediate steps should be taken to develop a comprehensive strategy to mitigate these threats. As a way forward, it is suggested:

- To ensure the coordinated efforts across the government a national coordinating agency should be created develop a new comprehensive strategy to secure Pakistan's information and communications networks.
- All the key players – public and private - should be involved in this process of developing comprehensive cyber strategy.
- The government should collaborate with industry, by developing public private partnerships, to find technology solutions that ensure our security.
- Investments should be made in the cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time. The government identify the organizations involved in cyber security research through out the country and support them.
- A national campaign to develop the awareness and digital literacy should be launched through out the country, from our boardrooms to our classrooms.

The News, a leading daily newspaper reported on June 30, 2021, "In a recent development, India is now ranked at No 10 at the Global Cyber Security Index, up from No 47 in 2019, as per a study by the United Nations. According to the study, the same index ranks Pakistan at No 79, foreign media reported."

We are living in the world of digital revolution and adopting a right strategy and swift implementation, will ensure our success in achieving the goal of creating Cyber Secure Pakistan.