Editorial

Wednesday, April 10, 2019

"CAB " Factor Faded

Many critic say, "Inclusion of Citizenship Amendment Bill (CAB) issue in the Election Manifesto is an insult to the people of the North East". But many in the BJP front are justifying the inclusion of CAB issue in the BJP party Manifesto saying that the reintroduction of the CAB which had failed to even table in the Rajya Sabha , thereby collapsing the Bill will do no harm to the North East Region including the state of Manipur.

The way the CSOs, Students' Bodies and other civil society organizations responded to the inclusion of the contentious CAB issue is also surprising. A new comer who missed the entire show of mass protest and uproar when the NDA regime passed the Contentious CAB Bill to the Lok - Sabha would definitely feel that the CSOs and the people of the region do not have much problem with the introduction of the CAB as none targeted the Bulls eye. Thanks to one group of CSO called PAM which boycotted the BJP for inclusion of CAB issue in the election Manifesto. If the issue of CAB is serious and people of the state vehemently opposed it then there is no reason to expect another uproar to the ruling BJP.

'It' didn't happen. Manipur sons of the soil who are cadres of the BJP and who had close affiliation with the BJP remain silent this time. What is more interesting is that civil society leader who had strongly opposed the contentious CAB during series of debate in public platform have today openly support the BJP candidate for the Inner Manipur Lok Sabha Poll scheduled to hold on April 18.

The people of the state had seen apprehension to the face of the Chief Minister at that time when there was public uproar in the state against the BJP's stand for passing of the Bill at Rajya Sabha. The Chief Minister even took credit of not tabling the CAB to Rajya Sabha saying that it is his government effort that the CAB was not tabled in the Rajya Sabha. Time and again the people of the state heard the Chief Minister N. Biren Singh saying that he will urge the center to insert a clause that might exclude North East Particularly the state of Manipur from the purview of the CAB even though everyone knows that the concept of inserting a clause to exclude the state from the purview of the Bill is next to impossible. The words of the Chief Minister might have been used time and again as he and his party may have thought that 60% to 70% of the people of the state have no idea of CAB. This is being assumed after hearing a BJP spokesperson said that CAB will not affect BJP as over 60 % to 70 % of the people of the state do not have the idea of what is there in CAB during a discussion hour at a local TV discussion programme.

Today, a BJP, MLA – Radhakishore openly said that CAB is the need of the country. He had openly said that BJP will surely re-introduce CAB if come to power.

It is now crystal clear that among others BJP is bringing back the contentious CAB Bill and convert it into law. The uproar and the criticism have been shut and now the BJP have the guts to come out in public in support of CAB. One wanders how the magic works. One wanders how a one time leader of a CSO openly supports the BJP candidate when he had many times criticized the Bill during discussion hour at Public platform.

The way the Indian election works is either on muscle and money power and not on the issues that matters the state of Manipur. Because every knows the fate of the state on what would happen if the contentious CAB is converted into law of the country.

Letters, Feedback and Suggestions to* 'Imphal Times' *can be sent to our e-mail : imphaltimes@gmail.com. For advertisement kindy contact: - 0385-2452159 (O). For time being readers can reach the office at Cell Phone No. 9862860745 for any purpose.

"Cyber Security"-the need of the hour.

By: Sanjenbam Jugeshwor Singh.

Computer security, Cyber security or information technology security (IT security) is the protection of computer system from theft or damage to their hardware, software or electronic data as well as from disruption or misdirection of the services they provide. The field is growing importance due to increasing reliance on computer system, the Internet and wireless networks such as Bluetooth and Wi-Fi and due to the growth of smart devices including smart phones, television and various tiny devices that constitute the Internet of things. Due to its complexity both in terms of politics and technology, it is also one of the major challenges of the contemporary world.

A vulnerability is a weakness in design, implementation, operation or internal control. Most of the vulnerabilities that have been discovered are documented in the common vulnerabilities and exposure (CVE) database. An exploitable vulnerability is one for which at least one working attack or exploit exist. Vulnerabilities are often hunted or exploited with the aid of automated tools or manually using customized scripts. To secure a computer system ,it is important to understand the attacks that can be made against it, and these threats can typically classified as(i) Backdoor in computer system ,a cryptosystem or an algorithm is any secrete method of bypassing normal authentication or security control (ii) Denial –of-service attacks(DoS)are designed to make a machine or network resource unavailable to its intended users(iii) Direct-access attacks, which is an unauthorized user gaining physical access to a computer is most likely able to directly copy data from it.(iv) Eavesdropping is the act of surreptitiously listening to a private conversation ,typically between hosts on a network.(v) Multivector, polymorphic attacks ,surfacing in 2017 ,a new class of multivector, polymorphic cyber threats .(vi) Phishing is the attempt to acquire sensitive information such as usernames, passwords and credit card details directly from users.(vii) Privilege escalation describes a situation where an attacker with some level of restricted access is able to without authorization ,elevate their privilege or access level.(viii) Social Engineering aims to convince a user to disclose secrets such as passwords ,card number etc.(ix) Spoofing is the act of masquerading as a valid entity through falsification of data such as IP address or username in order to gain access to information or resources that one is authorized to obtain.(x) Tampering describe a malicious modification of product.

Many people think of cybersecurity as a highly technical challenge, one that consumes the brain power of technical experts, however the general public plays a vital role in cybersecurity. If cybersecurity & cybercrime deterrence are not treated as priorities, the rate at which system and data are abused will continue to rise, further undermining the public's trust in technology. The growth in the number of computer systems and the increasing reliance upon them of individuals ,businesses ,industries and government means that there are an increasing number of system at risk, which may be financial system, utilities and industrial equipment, Aviation, Consumer devices ,Large corporations, Automobiles , Government, Internet of things and physical vulnerabilities, medical systems, energy sector etc. Serious financial damage has been caused by security breaches but because there is no standard model for estimating the cost of an incident, the data available is that which is made public by the organization involved. As with physical security, the motivations for breaches of computer security vary between attackers.

In computer security a countermeasure is an action, device, procedure or technique that reduces a threat, a vulnerability or an attack by eliminating or preventing it by minimizing the harm it can cause or by discovering and reporting it so that corrective action can be taken. Some common countermeasure are: Security by design, security architecture, Security measures, Vulnerability management, reducing vulnerabilities, Hardware protection mechanisms ,Secure operating systems, secure coding ,capabilities and access control lists, end user security training, response to breaches. Incident response is an organized approach to addressing and managing the aftermath of a computer security incident or compromise with the goal of preventing a breach or thwarting a cyber-attack. Incident response planning allows an organization to establish a series of best practices to stop an intrusion before it causes damage. Four key components of computer security incident response plan are: preparation, detection & analysis, containment, eradication & recovery and post incident activity. Some of the important components of Network security are- Anti-virus and anti-spyware, Firewall to block unauthorized access to your network, intrusion prevention system (IPS) to identify fast-spreading threats such as zero day or zero hour attacks and Virtual Private networks((VPNs) to provide secure remote access.

International legal issues of cyber-attacks are complicated in nature. There is no global base of common rules to judge and eventually punish, cybercrimes and cybercriminals and cyber security firms or agencies do locate the cybercriminals behind the creation of a particular piece of malware or form of cyber-attack ,often the local authorities cannot take action due to lack of laws under which to prosecute. The role of government is to make regulations to force companies and organizations to protect their systems, infrastructure and information from any cyber-attacks but also to protect its own national infrastructure such as the national power grid. In India some provisions for cyber security have been incorporated into rules framed under the Information Technology Act 2000.The National Cyber Security policy 2013 is a policy framework by Ministry of Electronics and Information Technology (MeitY) which aims to protect the public and private infrastructure from cyber-attack and safeguard information such as personal information (of web user), financial and banking information and sovereign data. CERT-In is the nodal agency which monitors the cyber threats in the country. The Indian Companies Act 2013 has also introduced cyber law and cyber security obligations on the part of Indian directors. Some provisions for cyber security have been incorporated into rules framed under the Information Technology Act 2000 updated in 2013.On the top of all these legality, what we can do simply is educate yourself and others on the preventive measures you can take in order to protect yourself as an individual or as a business. ***Some of the important tips about cyber security that we common people can do are: become vigilant when browsing websites, flag and report suspicious e-mails, never click on unfamiliar links or ads, use a VPN whenever possible, ensure websites are safe before entering credentials, keep antivirus/ application system up to date, use strong passwords with 14+ characters***.

Writer can reach to:sjugesheow7@gamail.com or WhatsApp No:96112891339.

'Women back then would basically go, "Well, if I don't do programming, what else will I do?"

Courtesy The Wire
By : Clive Thompson

Elsie Shutt learned to code during her college summers while working for the military at the Aberdeen Proving Ground, an Army facility in Maryland. In 1953, while taking time off from graduate school, she was hired to code for Raytheon, where the programmer work force "was about 50 percent men and 50 percent women," she told Janet Abbate, a Virginia Tech historian and author of the 2012 book "Recoding Gender." "And it really amazed me that these men were programmers, because I thought it was women's work!"

When Shutt had a child in 1957, state law required her to leave her job; the '50s and '60s may have been welcoming to full-time female coders, but firms were unwilling to offer part-time work, even to superb coders. So Shutt founded Computations Inc., a consultancy that produced code for corporations. She hired stay-at-home mothers as part-time employees; if they didn't already know how to code, she trained them. They cared for their kids during the day, then coded at night, renting time on local computers. "What it turned into was a feeling of mission," Shutt told Abbate, "in providing work for women who were talented and did good work and couldn't get part-time jobs." Business Week called the Computations work force the "pregnant programmers" in a 1963 article illustrated with a picture of a baby in a bassinet in a home hallway, with the mother in the background, hard at work writing software. (The article's title: "Mixing Math and Motherhood.")

By 1967, there were so many female programmers that Cosmopolitan magazine published an article about "The Computer Girls," accompanied by pictures of beehived women at work on computers that evoked the control deck of the U.S.S. Enterprise. The story noted that women could make $20,000 a year doing this work (or more than $150,000 in today's money). It was the rare white-collar occupation in which women could thrive. Nearly every other highly trained professional field admitted few women; even women with math degrees had limited options: teaching high school math or doing rote calculations at insurance firms.

"Women back then would basically go, 'Well, if I don't do programming, what else will I do?' " Janet Abbate says. "The situation was very grim for women's opportunities."

[The Yoda of Silicon Valley]

If we want to pinpoint a moment when women began to be forced out of programming, we can look at one year: 1984. A decade earlier, a study revealed that the numbers of men and women who expressed an interest in coding as a career were equal. Men were more likely to enroll in computer-science programs, but women's participation rose steadily and rapidly through the late '70s until, by the 1983-84 academic year, 37.1 percent of all students graduating with degrees in computer and information sciences were women. In only one decade, their participation rate more than doubled.

But then things went into reverse. From 1984 onward, the percentage dropped; by the time 2010 rolled around, it had been cut in half. Only 17.6 percent of the students graduating from computer-science and information-science programs were women.

One reason for this vertiginous decline has to do with a change in how and when kids learned to program. The advent of personal computers in the late '70s and early '80s remade the pool of students who pursued computer-science degrees. Before then, pretty much every student who showed up at college had never touched a computer or even been in the room with one. Computers were rare and expensive devices, available for the most part only in research labs or corporate settings. Nearly all students were on equal footing, in other words, and new to programming.

Once the first generation of personal computers, like the Commodore 64 or the TRS-80, found their way into homes, teenagers were able to play around with them, slowly learning the major concepts of programming in their spare time. By the mid-'80s, some college freshmen were showing up for their first class already proficient as programmers. They were remarkably well prepared for and perhaps even a little jaded about what Computer Science 101 might bring. As it turned out, these students were mostly men, as two academics discovered when they looked into the reasons women's enrollment was so low.

One researcher was Allan Fisher, then the associate dean of the computer-science school at Carnegie Mellon University. The school established an undergraduate program in computer science in 1988, and after a few years of operation, Fisher noticed that the proportion of women in the major was consistently below 10 percent. In 1994, he hired Jane Margolis, a social scientist who is now a senior researcher in the U.C.L.A. School of Education and Information Studies, to figure out why. Over four years, from 1995 to 1999, she and her colleagues interviewed and tracked roughly 100 undergraduates, male and female, in Carnegie Mellon's computer-science department; she and Fisher later published the findings in their 2002 book "Unlocking the Clubhouse: Women in Computing."

What Margolis discovered was that the first-year students arriving at Carnegie Mellon with substantial experience were almost all male. They had received much more exposure to computers than girls had; for example, boys were more than twice as likely to have been given one as a gift by their parents. And if parents bought a computer for the family, they most often put it in a son's room, not a daughter's. Sons also tended to have what amounted to an "internship" relationship with fathers, working through Basic-language manuals with them, receiving encouragement from them; the same wasn't true for daughters. "That was a very important part of our findings," Margolis says. Nearly every female student in computer science at Carnegie Mellon told Margolis that her father had worked with her brother — "and they had to fight their way through to get some attention."

(To be Continued)