Editorial

Together lets' save the future

Consider a building with a few broken windows. If the windows are not repaired, the tendency is for vandals to break a few more windows. The proverb 'A stitch in time saves nine' is worth remembering here.

Eventually, they may even break into the building, and if it's unoccupied, perhaps become squatters or light fires inside. Or consider a pavement. Some litter accumulates. Soon, more litter accumulates. Eventually, people even start leaving bags of refuse from take-out restaurants there or even break into cars. If the concept is to be applied to the law and order situation in our society with special emphasis to the prevailing system of administration and governance, one would find the same psychological response to the prevailing situation. This very social phenomena is termed the Broken Window Theory - introduced by James Q. Wilson and George L. Kelling in an article titled Broken Windows, in the March 1982 The Atlantic Monthly following an experiment by Philip Zimbardo, a Stanford psychologist who tested the theory in 1969. Unsurprisingly for many, the test concluded that vandalism, or for that matter, most forms of social disturbances occurs much more quickly as the community generally seems apathetic.

Similar events can occur in any civilized community when communal barriers – the sense of mutual regard and obligations of civility – are lowered by actions that suggest apathy. In other words, the theory posits that the prevalence of disorder creates fear in the minds of citizens who are convinced that the area is unsafe. This withdrawal from the community weakens social controls that previously kept criminals in check. Once this process begins, it feeds itself. Disorder causes crime, and crime causes further disorder and crime. A lot of social discrepancies- between the accepted social norms and the ground reality can be explained based on this theory. The snowballing effect of corruption, favoritism, unrest and elitism being increasingly experienced by the general public in the state can be understood more clearly and objectively when one understands the psychology behind the cause of such undesirable social occurrences. But understanding the cause is not the panacea to the festering problem, it is rather the beginning of a long and tedious process of reforms and redressals which should be pursued relentlessly. But the task at hand is easier said than done.

The present system of administration and governance which has been consciously shaped and engineered to comply and conform to the interests of a precious few having access to power and connections, with the added bonus of having in place various mechanisms to protect and cover the nefarious activities and conniving characteristics of those fortunate few, needs to be pulled down and a radical system to administration and governance has to be drawn up be implemented without further ado. In short, an overhauling of the deep rooted social evils and malpractices that has been inextricably intertwined with the present system is the need of the hour.

Its times that people make effort to change the system - Yes parliament election is just few days to go. Together lets make a change.

Need For India's Veto Power at UNO

By- L. Nehkholien Haokip Kuki

The much waited and cherish dreams for India's to be the Veto power at United Nations Organisation(UNO) can be cited after Phulwana attacked by Pakistan based Jaish- e-Mohammad(JeM) terrorist master mind behind the Pulwana district of Kashmir India attacked in which 40 braved soldiers of Central Reserve Police Force(CRPF) had lost their life leaving their dear ones.

Jaish-e-Mohammad(JeM) to sanction their asset and to declare as terrorist organization at the UNO has been blocked by China the fourth times under the Veto power, why? Even India supported China candidature when needed for Veto power at UN, P-5 or UNSC. But the Veto powers like US, Britain and France back India sponsoring JeM, LeT and it supporter India historical neighbour Pakistan for economic embargo or US F-16's already supplied to Pakistan that uses one of the largest democratic country India since, 1947 when Pakistan got independence.

What's the needs for India's - a must to become one of the members of Veto powers country, P-5 or UNSC at UNO future expansion else's terrorists sponsoring by Pakistan could not be put into action and passed resolution at the UNO to be Vetoed by China. The clarion calls for Veto power countries or the P-5 is to support India's berth for Veto power at the UN as a responsible and country to counter the terrorist directly or indirectly.

The need of the hour lies the expansion of UNO Veto power expansionism one from Asia continent and another one from Africa continent and also another one from Oceania so as to deals with terrorists and the world peaceful co-existence amongst its member countries. Lastly the charters of UNO can be put into action and sanctioned or economic embargo to any country like Pakistan sponsoring terrorist likes Jaish-e-Mohammad(JeM) and Lasker-e-Toiba (LeT) organisations that effects India's security concern throughout the world.

"Cyber Crimes"-Crimes by finger tips.

By: Sanjenbam Jugeshwor Singh.

Cyber Crime or Computer oriented Crime is the crime that involved a computer and a networks. The computer may have been used in the commission of a crime or it may be the target. Cybercrime can be defined as: *Offences that are committed against individual or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm or loss to the victim directly or indirectly using modern telecommunication networks such as Internet (networks including chat rooms, e-mails, notice board and groups) and mobile phones (Bluetooth, SMS, MMS).*

Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high profile, particularly those surrounding hacking, copyright infringement, unwanted mass surveillance, sextortion, child pornography and child grooming. There are also problem of privacy when confidential information is intercepted or disclosed lawfully or otherwise. Internationally both governmental and non-state actor engage in cybercrimes including espionage, financial theft and other cross-border crimes. Cybercrimes crossing international border and involving the actions of at least one nation state is sometimes referred to as Cyberwar fare.

A report sponsored by **McAfee** published in 2014 estimated that the annual damage to the Global economy was \$445 billion. Approximately \$1.5 billion was lost in 2012 to online credit and debit Card fraud in the US. In 2018 a study by **Center for Strategic and International Studies (CSIS)** in Partnership with **McAfee** concludes that close to \$600 billion, nearly 1% of global GDP is lost to Cybercrime each year. Computer crime or cybercrime encompasses a broad range of activities. Any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which cause loss is known as Computer Fraud. Other forms of fraud may be facilitates using computer system, including Bank fraud, Carding, identity theft, extortion and theft of classified information. A variety of internet scams, many based on phishing and social Engineering target consumers and businesses. An act of terrorism committed through the use of cyberspace or computer resources is generally defined as Cyber terrorism. As such a simple propaganda piece in the Internet that there will be bomb attack during holidays can be considered as cyber terrorism. Cyber extortion occurs when website- email server or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attack and offer protection. Perpetrators typically use a distributed denial of service attack. However other cyber extortion techniques exist such as doxing extortion and bug poaching. Cyber warfare is not the least to mention. The U.S Dept. of Defense (DoD) notes that the cyberspace has emerged as a national level concern through several recent event of geostatic significance. Among those are included the attack on Estonia's infrastructures in 2007, allegedly by Russian hackers. Russian again allegedly conducted cyber-attacks, this time a coordinated and synchronized kinetic and non-kinetic campaign against Georgia. These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computer have – which explains how unprepared society and the world in generals in combating these crimes. There are numerous crime of this nature committed daily on the internet. Crimes that primarily target computer networks or devices includes Computer Viruses, denial of service attacks, malware (malicious code).

When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise .Human weakness are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. Crimes that use computer networks or devices to advance other end includes: fraud and identity theft, information warfare, phishing scams, spam (the unsolicited sending of bulk e-mail for commercial purposes). The content of the websites and other electronic communication may be distasteful, obscene or offensive for a variety of reasons. Whereas content may be offensive in a non-specific way, harassment, direct obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation . These offences occurs in the chat rooms through newsgroups and by sending hate-email to interested parties. Harassment on the internet also includes revenge porn. Dark net markets are used to buy and sell recreational drugs online. Some drug traffickers used encrypted messaging tools to communicate with drug mules.

As technology advances and more people rely on the internet to store sensitive information such as banking or credit cards information, criminals increasingly attempts to steal that information. Cybercrime is becoming more of threat to people across the world. Raising a weakness about how information is being protected and the tactics criminals use to steal that information continue to gain in importance.

The Evolution of the Skills Gap Requires 21st Century Solutions

Courtesy The Were **By : Cheryl A. Oldham**

Both the White House and business community agree that the skills gap, a source of longstanding debate in the United States, is real and requires action. There is a bloc of opinion that refuses to acknowledge that the skills gap has ever been a legitimate issue; some would say it simply doesn't exist.

Matthew Yglesias of Vox and Matt O'Brien of the Washington Post, are among many who have recently spotlighted and written about a new research paper presented in January at the American Economics Association's annual conference. They make the argument that because employers change their requirements for jobs to directly deal with high unemployment and the growing volume of resumes joblessness produces, a skills gap does not exist. This new research is not inaccurate, but the lines critics are trying to draw from it are misleading, and false.

While it is accurate that, in times of high unemployment, employers add more credentials and qualifications to job descriptions, this practice is only indirectly related to the skills gap. Employers historically add these requirements because it reduces the number of applications they get, narrowing the field to those applicants who are most qualified for the jobs available. This is an outdated practice that may make it easier to filter through applications, but it will not guarantee a hire with the right skill-sets aligned to the employer's talent needs.

Over the last decade we have seen the challenges associated with the skills gap gain new dimensions given changes in workplace development, jobs, and in-demand skills in the 21st century economy. One significant evolution is that the skills gap is no longer just a conversation about a lack of specialized skills available in the talent marketplace. It has evolved into a conversation about the underlying cracks in the foundation. In dissecting the skills gap, we've identified that employers struggle to communicate their hiring needs to the education community. We also know that traditional education and career pathways weren't designed to develop skills for a fast-changing market or to match the speed of changing industry requirements.

Maura Reynolds, senior editor for Politico, reports that the education community needs disruption. What this economy needs is a consistent and high-quality way for the education community to effectively collaborate with employers to develop talent that aligns with the needs of our quickly changing economy.

In line with a recent report from the World Economic Forum, Strategies for the New Economy, there are a few critical shifts that all stakeholders of the talent marketplace must make together, many of which are already in development:

Map the skills content of jobs and make it open, machine-readable data to achieve real-time signaling of labor market changes.

Design coherent and portable credentials.

Develop a new approach to talent management that includes effective partnerships and real career pathways.

Align skills taxonomies between the business and education communities. These approaches require employers to have a little more skin in the game, but it's worth it. When a worker's skills are more aligned to the needs of the market, they are more quickly hired, they are more valuable to the employer, and they are better positioned for future promotion.

In both prosperous and challenging times, there is an ongoing gap that stands in the way of opportunity for many. Maybe we need to stop calling it the skills gap, or we need to collectively redefine what the gap is. No matter what we call it, we can all agree that the time for solving it is now.