A Brief Report

Third BN Mullick Memorial Lecture, August 31, 2024

Introduction

The third BN Mullick Memorial Lecture was organised jointly by ARSIPSO and the IIC on August 31,2024 to honor the legacy of Mr. Malik, a distinguished intelligence officer and former director of the Intelligence Bureau. Known for his pivotal role in shaping India's national security framework, Mr. Mullick's contributions to the country were highlighted, with special attention to his service as a Principal Advisor to Prime Minister Nehru for security matters and his long tenure as Director of AP. He was awarded the Padma Bhushan in 1964. His significant publications, including *My Years with Nehru: The Chinese Betrayal*, and his leadership in security were acknowledged. The memorial event was graced by his granddaughter, Ms. Kamla Bhattacharya.

The lecture's focus was "Cybersecurity for the Common Man," a topic of growing concern in today's digital age. Esteemed guest Adv Dr. Muktesh Chander, a renowned expert in cybersecurity, led the discussion, Dr. Muktesh Chander is leader in the field of cybersecurity, with a notable academic background and professional accomplishments. His credentials include a Ph.D. in Information Security Management, a law degree, and several other qualifications related to cybersecurity. He has held prestigious positions, including **Special CPD** and **DGP**, and is a life member of the Computer Society of India. During the lecture. Dr. Muktesh Chander shared his knowledge on various dimensions of cybersecurity and its impact on individuals and the nation.

Detailed Proceedings

Dr. Muktesh Chander began his address by outlining the three main dimensions of cybersecurity: individual, organizational, and national security. He emphasized the increasing risks of cyber-attacks at all levels, particularly focusing on how common individuals fall prey to cyber frauds, malware attacks, and online scams. His presentation provided critical insights into how these risks are escalating, driven by the rapid adoption of digital tools without adequate security measures.

Cyber Threats to Individuals: Dr. Chander addressed the pressing issue of cybersecurity for common citizens. He emphasized that with the increasing dependence on digital technologies such as smartphones, laptops, and online platforms, individuals are highly vulnerable to cyber-attacks. These attacks often come in the form of:

- **Phishing scams**, where unsuspecting users are tricked into providing sensitive information like banking details.
- **SIM swapping**, a dangerous tactic where criminals replicate SIM cards to intercept One-Time Passwords (OTPs).

- **Fake helplines and websites**, which lure individuals into fraudulent schemes under the guise of legitimate services.
- **Social media exploitation**, where personal information is used to manipulate and defraud individuals.

Organizational Security: Dr. Chander further highlighted the dangers faced by businesses and government institutions from sophisticated cyber-attacks. He referenced recent cyber incidents involving major Indian organizations and warned about the potential financial and reputational losses organizations can suffer due to inadequate cybersecurity protocols. Some key threats to businesses include:

- **Data breaches**, where sensitive corporate data is stolen or manipulated.
- **Malware attacks**, which can cripple entire systems and lead to huge financial losses.
- **Ransomware**, where attackers encrypt organizational data and demand a ransom for its release.

He stressed that the lack of awareness and preparedness within organizations often leads to significant financial and reputational damage. Many companies, especially small and medium enterprises, fail to implement adequate security measures, leaving them exposed to cyber-attacks. Thus, the need for continuous employee training and regular cybersecurity audits was underscored to mitigate these risks.

National Security Implications: Dr. Chander also explored the intersection of cybersecurity and national security, emphasizing that large-scale cyber-attacks have the potential to disrupt national infrastructure. The broader threats to national infrastructure from cyber-attacks were examined. He cited examples where cybercriminals have targeted government organizations, potentially compromising national security. The advent of technologies like **Artificial Intelligence** (AI) and **Deepfakes** has further complicated the landscape, making it harder to distinguish between legitimate and fraudulent activities. He outlined the role of cybersecurity in safeguarding critical national assets and the challenges faced by law enforcement in addressing these threats.

He pointed towards the challenges faced by **law enforcement agencies** in dealing with cybercrimes. He explained that while the government has made strides in cybersecurity, more needs to be done to create an integrated approach that combines public awareness, corporate responsibility, and government action.

Throughout the lecture stressed the importance of proactive measures such as awareness and personal responsibility in maintaining cyber safety. He pointed out that many people remain unaware of basic cybersecurity practices, often leading to catastrophic consequences.

Recommendations

At the end of the lecture, Dr. Chander offered several key recommendations to improve cybersecurity at all levels:

1. **Public Awareness Campaigns**: Initiatives to educate the public about basic cybersecurity practices, such as recognizing phishing attempts, securing personal devices, and not sharing sensitive information online, should be intensified. He suggested leveraging media and educational institutions to spread this awareness.
2. **Organizational Accountability**: He recommended that companies, particularly those handling sensitive data, must invest in robust cybersecurity frameworks. This includes regular training sessions for employees, the use of advanced encryption methods, and the establishment of incident response teams to handle cyber-attacks.
3. **Improving Law Enforcement Capabilities**: He emphasized the need for specialized training for law enforcement officers to keep up with evolving cybercrime tactics. More resources should be allocated to create efficient cybercrime units within police forces that can respond quickly and effectively to threats.
4. **Development of National Cybersecurity Policies**: Dr, Chander advocated for the constant updating of national policies to address emerging threats, such as AI-driven cyber-attacks and ransomware. He also stressed the importance of international cooperation in tracking and prosecuting cybercriminals operating across borders.
5. **Personal Responsibility for Cyber Safety**: Individuals need to take responsibility for their own digital security by using strong passwords, regularly updating software, and installing reliable antivirus solutions on their devices.

Conclusion

The third BN Mullick Memorial Lecture not only honored the legacy of Mr. Malik but also provided valuable insights into the current cybersecurity challenges faced by individuals, organizations, and nations. Dr. QUESTION's comprehensive and engaging lecture shed light on the vulnerabilities in our increasingly digital world and underscored the need for collective action to protect against cyber threats. The discussions and recommendations made during the event stressed the importance of awareness, preparation, and vigilance in safeguarding our digital lives. The lecture concluded with a sense of urgency for everyone, from individuals to governments, to take proactive steps toward improving cybersecurity.