Center for Global & Strategic Studies, Islamabad

National Security Division, Government of Pakistan

Seminar Report

CYBER SECURE PAKISTAN POLICY FRAMEWORK

"CGSS is a Non-Profit Institution with a mission to help improve policy and decision-making through analysis and research"

Printed in Pakistan

Published in April, 2018

ISBN 978 969 7733 17 0

CGSS
Center for Global & Strategic Studies

3rd Floor, 1-E, Ali Plaza, Jinnah Avenue, Islamabad, Pakistan

Tel: +92-51-8319682

Email: **info@cgss.com.pk** Web: **www.cgss.com.pk**

Seminar Report

"Cyber Secure Pakistan – Policy Framework"

Organized by
Center for Global & Strategic Studies, Islamabad
In collaboration with
National Security Division, Government of Pakistan
at
Margala Hotel, Islamabad

Participants

The Seminar was attended by almost 300 participants including government representatives, retired senior armed forces officers, diplomats, and cyber experts from across the country and individuals from public and private entities.

Host	**Lieutenant General Muhammad Zahir Ul Islam HI (M), (Retd) - Chairman Center for Global & Strategic Studies (CGSS)**
Guest Speakers	**Lieutenant General Nasser Khan Janjua, HI (M), (Retd) – National Security Advisor, PM Secretariat, Islamabad**
	Mr. Syed Iftikhar Hussain Babar - Secretary National Security Division, Government of Pakistan
	Mr. Ammar Jaffery - Director General, Center of Information Technology (CIT)
	Mr. Tariq Malik - Former Chief Technology Officer, GHQ
	Mr. Mudassar Hussain - Member Telecom, Ministry of Information Technology, Government of Pakistan
	Dr. Muddassar Farooq - Chief Technology Officer, Neomantix
	Mr. Irfan Ur Rehman - Former Head of Cyber Security Operations at PTCL
	Mr. Yusuf Hussain - Chairman IGNITE – National Technology Fund, Ministry of Information & Technology

Introduction of the Speakers

Lieutenant General Nasser Khan Janjua, HI(M), (Retd), - National Security Division, Government of Pakistan

General Nasser Khan Janjua is the National Security Adviser of Pakistan. He has been through some vast experiences during his long military career, spread over nearly four decades. He possesses a unique insight into challenges confronting, National and International Peace and Security. The General Officer served Pakistan Army in various capacities. He Commanded his Regiment in Gilgit and a Brigade in Siachin and led the counter terrorism Operation, "Operation RAH-E-HAQ" while commanding an Infantry Division in Swat. His last position was Commander Southern Command, where he played a vital role, in eradicating extremism, militancy, terrorism and insurgency. In addition to distinguished Command assignments, he has also been, Chief of Staff of a Strike Corps, Director Military Operations, Chief of Staff of Southern Command, Vice Chief of the General Staff and President National Defence University. In recognition of his meritorious services, Chief of Army Staff and Prime Minister of Pakistan have collectively chosen General Nasser Janjua as National Security Advisor.

Mr. Syed Iftikhar Hussain Babar - Secretary National Security Division, Government of Pakistan

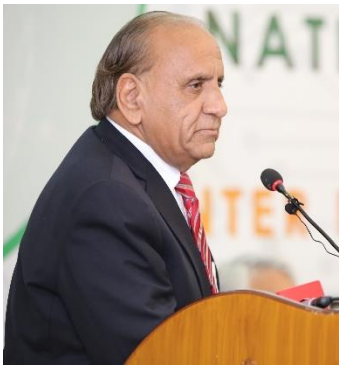
Mr. Syed Iftikhar Hussain Babar, Secretary National Security Division (NSD), Government of Pakistan has rich experience of provincial and federal government, field and secretariat assignments. He has held many prominent positions a few of which include Additional Secretary in the Prime Minister Secretariat and in the Economic Affairs Division in addition to Managing Director Overseas Pakistanis Foundation. He has also

served as Secretary Board of Investment, and Federal Secretary Wafaqi Mohtasib.

Mr. Mudassar Hussain – Member Telecom, Ministry of Information Technology, Government of Pakistan

Mr. Mudassar Hussain is Member Telecom, Ministry of Information Technology, Government of Pakistan. Prior to joining MoITT, he was working as the Telecom Policy & Regulatory Consultant with Ufone. As Director in MoITT he has served on the Boards of the National Telecommunications Corporation, the Telecom Foundation and the National Radio Telecommunications Corporation.

Mr. Ammar Jaffery – Director General, Center of Information Technology (CIT)



Mr. Ammar Jaffery is Director General, Center of Information Technology (CIT). Mr. Jaffery has been the Former Additional Director General FIA and Pioneering Head of NRC3. Currently, he is heading the initiative of cyber secure Pakistan and engaged in awareness campaigns on Cyber Security locally and internationally.

Mr. Tariq Malik – Former Chief Technology Officer, GHQ

Mr. Tariq Malik served as the Former Chief Technology Officer GHQ. Mr. Tariq Malik, is currently working as Chief Technical Advisor, United Nations Development Program (UNDP), and has been the former CHAIRMAN of the National Database and Registration Authority (NADRA) Pakistan. Prior to joining UNDP, he held the position of a Senior Technical Consultant at World Bank. He was a member of the core team who helped to initiate the worldwide 'ID for Development' (#ID4D) Program.

Mr. Yusuf Hussain- Chairman IGNITE – National Technology Fund, Ministry of Information & Technology

Mr. Yusaf Hussain is the Chairman IGNITE- National Technology Fund, Ministry of Information and TECHNOLOGY. He recommends policy guidelines and future strategy to the federal government about development of Cyber security Mechanisms.

Dr. Muddassar Farooq - Chief Technology Officer, Neomantix

Dr. Mudassar Farooq is Chief Technology Officer at Neomantix. Mr. Mudassar Farooq has remained Professor and Dean of Institute of Space Technology, (IST). Previously, he was professor and Vice Chancellor, Muslim Youth University. Sir, I invite you to share your expert opinion with all of us.

Mr. Irfan Ur Rehman – Former Head of Cyber Security Operations at PTCL

Mr. Irfan ur Rehmaan served as the Former Head of Cyber security operations at PTCL. Mr. Irfan ur Rehman is highly experienced in Information security, Governance and Risk Assessment. Currently, he is engaged in a telecom company, Etisalat Pakistan (PTCL) as Senior Manager cyber security Operations Islamabad centre.

Opening Remarks by

Lieutenant General Muhammad Zahir Ul Islam HI (M), Retd – Chairman CGSS

General Zahir (Retd) commenced his opening remarks, by extending his gratitude to the worthy members of the panel for the seminar and hoped for the session to be highly informative for the audience.

In today's world, we are totally dependent on the cyber-space, which is primarily the electronic communication. Electronic communication holds importance in every aspect of our lives. It is part of the governance, economy and defense. Being a necessity, it presents certain challenges. Challenges, of course, are in the realm of making the cyber-environment as secure as possible for the security of the country. As Pakistan develops its ability in the cyber-space, there are countries that are ready to break the security and penetrate into our cyber-space to get the information, which is critical for Pakistan's security. He concluded his remarks by stating that the upcoming speakers will recommend and discuss a strategy that will help protect Pakistan's interests against the threats posed by cyber-crime. The discussions will then help develop a policy framework, which will be presented and incorporated by the national security division in developing a national security policy.

Opening Address

Mr. Syed Iftikhar Hussain Babar

Secretary National Security Division, Government of Pakistan

Importance of Cyber Security

The Secretary NSD commenced his address by thanking the panelists and the audience for participating in the seminar. The National Security Division (NSD) decided upon conducting a seminar on the threats posed to cyber-security after the visit of a certain cyber-security agency last month. Crucial information was shared among the two parties, realizing the grave importance the issue has to itself. The panelists will thus extend their vast knowledge on challenges and threats of the cyber-space in an endeavor to provide necessary solutions to help Pakistan fight the threats posed by all spheres of cyber-security.

He further stated that wars have long been fought on land, air and at sea. Future wars, however, will be fought on cyber space. Cyber warfare is internet-based which include politically motivated attacks on information and information systems. Cyber warfare attacks can disable official websites and network, disrupt essential services, even steal, alter or destroy classified data and cripple financial systems among many other possibilities. Cyber insecurity is now established as a serious unconventional threat.

An electronic army of simple hackers using computers to gain unauthorized access to the computers of the target country with the objective of crippling the target country's networks is the process of cyber-warfare. Today, an embedded computer in every modern device like our mobile phones, exposes each and every one of us to cyber-threats. The image of a country's electronic army taking over our plants, refineries, pipelines, airlines, banks even nuclear reactors, is a horrifying one.

In 2010, online hackers named as 'India Cyber Army' attacked 36 of Pakistan's government websites. In 2013, another clan of Indian hackers sabotaged the Election Commission website of Pakistan. In retaliation, a group of Pakistan's hackers named as 'True Cyber Army' sabotaged 1059 websites of India's electoral bodies. On September 18, 2016, a militant attacked India's army brigade in Uri, leading to a full-scope cyber war between hackers from both the countries.

These incidents make us realize that the world we live in has changed and it has changed fast. The management of data is 'key' to prevent cyber-attacks. In the past, physically access files led to data manipulation. Today, however, a person sitting millions of miles away can access all forms of data in an instant. Cyber space knows no geographical limitations or boundaries. Data that is compromised and data that is sensitive can influence our lives and security. The 'WannaCry virus' which made the headlines recently, is a ransom-ware that makes data unreadable. Thus, the protection of data is as important as the protection of human lives. Our governments and various state intuitions have stored sensitive data. While it is safe to assume that Pakistan's sensitive agencies protect the data and take steps to ensure its integrity, it is not always true. The possibilities of the data with the Federal Board of Revenue or the NADRA, or the Pakistan intelligence

agencies being hacked, can be excessively worrisome to Pakistan. The seminar thus aims to raise awareness on this issue and the choices we have as users in the cyberspace.

He further stated that the threat of cyber warfare is real to mention many examples. In 2009, Indian Army's Military Operations Directorate conducted a war-game code-named Divine Matrix. In 2010, Indian National Security Advisor drafted an offensive cyber warfare strategy that brought all the intelligence agencies and RAW on the same page. In 2010, Stuxnet, an American-Israeli malicious computer worm brought down one of Iran's uranium plant in Isfahan province. In 2012, Shamoon, an Iranian linked worm attacked Saudi Aramco. In 2015, Chinese hackers pillaged secret details of Lockheed Martin's F35 stealth aircraft. On 9th December 2016, US President Barrack Obama ordered a review of a US election related serious cyber-attacks by Russia.

The prediction is that by 2021, the global annual cybercrime cost will double to 6 trillion dollars every year. Cyber security market will rise to 101 billion dollars in 2018 and will become 170 billion dollars by 2020. He also enlightened the audience with a list of top five countries, with cyber warfare capabilities, namely USA, UK, Russia, China and Israel.

To achieve the status of cyber readiness, Pakistan needs to address areas of instant response to counter the threat. Greater investments in cyber research and development, capacity and skill development are required to achieve cyber-security. Concerned organizations of the civil and military dimension are making tangible efforts in developing cyber security capabilities. Pakistan's Ministry of IT is working day and night to formulate the Prevention of Electronic Crimes Act, 2016 legislated to prevent unauthorized acts with respect to information systems, related offences as well as mechanisms for their prosecution.

Talking about national security means talking about the security of 200 million civilians and protecting the sovereignty of a country, strategically located and economically emerging.

Concluding the remarks, the secretary NSD stated that Pakistan presently is facing the menace of both terrorism and warfare, thus a cyber-security strategy is an integral part of national security policy. Cyber security needs to be ensured in a coordinated manner through cooperation among all relevant agencies, interconnecting their infrastructure

and services in cyber space. Pakistan must establish its foothold in cyber-space and formulate its state policy before the world further enhances its capabilities.

He ensured the audience that National Security Division serves as a secretariat for National Security Committee. The recommendations of this seminar will be processed and put up for consideration before the national security committee, which is the highest policy making and decision making body on the security related issues at national level presided over by the Prime Minister of Pakistan.

Speaker 1:

Dr. Muddassar Farooq

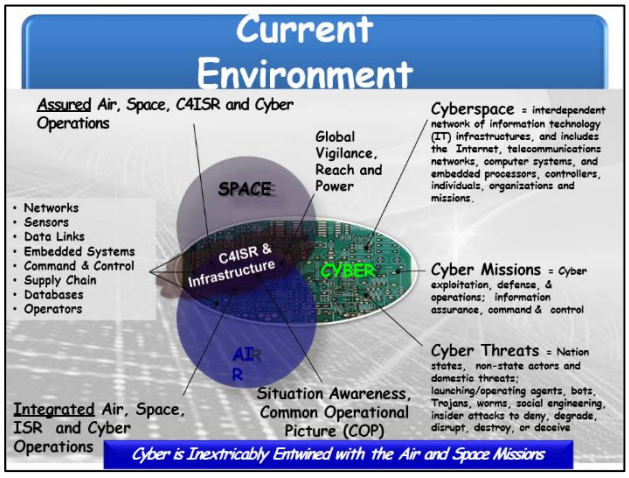
Chief Technology Officer, Neomantix

Cyber Warriors: An elite cyber-security unit is the future of Pakistan

Dr. Muddassar commenced his speech by stating that cyber is consisted of two things, the hardware/software and the human mind. It is thus important that the security provided to the people of Pakistan is significant. If there is a massive mega-infrastructure and the managers are ordinary human beings, then the cyber-secure system created will not be state of the art. Therefore, there is a need to align the best infrastructure with the best intellectual mind in the country. The foundation of the cyber security is based on the concepts such as:

1. Information security
2. Data privacy
3. Identity theft
4. Cyber-crime
5. Cyber-terrorism
6. Cyber warfare

The speaker set the focus for his speech specifically on cyber-terrorism and cyber-warfare. Sharing his experience from last year, as the Dean of Institute of Space & Technology, he mentioned that the SPD wanted to have a Cyber-Security Vision for strategic organizations and so asked the speaker to help. After reviewing 30-40 Cyber Security Vision Documents, he



found out that US' Airforce Cyber Security Vision 2025 is one of the best documents to refer. It covers aspects of space, air, infrastructure and the modern way of covering all the domains of satellite communications, regular network communication or hardware/infrastructure.

The document is mainly focused on the need to forecast future threats, mitigate vulnerabilities, enhance the industrial base, and develop the operational capabilities and cyber workforce necessary to assure cyber advantage across all Air Force mission areas. Furthermore, to create an integrated, Air Force-wide, near-, medium- and far-term science and technology (S&T) vision to meet or exceed air force cyber goals and, where possible, create revolutionary cyber capabilities to support core air force (AF) missions. It identifies state of the art and best practices in government and private sector and analyzes current and forecasted capabilities, threats, vulnerabilities, and consequences across core missions to identify critical S&T gaps. Moreover, it articulates AF near (FY11-16), mid (FY16-20) and long (FY21-25) term S&T to fill gaps, indicating where AF should lead, follow, or watch. It also addresses cyber S&T across all Air Force core missions and functions (air, space, C4ISR) comprehensively including policy as well as DOTMLPF considerations and engage different partners from industry, academia, national labs FFRDC and government. Cyber security cannot be overlooked in any field be it military, intelligence or economy. A cyber-mission thus should be drafted with utmost clarity.

US Air Force document further states that future Air-force fighters will be two guys rather one i.e. one the fighter pilot and other a cyber-security warrior, who will be sitting in a building trying to hack into enemy jets and gaining relative control over them. Controlling the avionics and electronics of a fighter jet can dismantle the pilot entirely. The stated technology is the landmark objective of cyber-warrior today. Today, developing such a capability is the central pillar of US future fighter air-crafts.

He further stated that Iran's nuclear power plant attacked by the Stuxnet worm proved that cyber-threats need to be addressed competitively. The Stuxnet worm installed itself in the nuclear plant's PLC (Programming Logic Controller) computer-controlled system and caused a change in the rotational speed of machinery making the nuclear plant fusion center spin uncontrollably, up until it exploded. Explaining the different dimensions of cyber-conflict, he said the difference between Cyber-warfare and Cyber-terrorism is very small. The state's involvement in the cyber-space is deemed as cyber-security/cyber-warfare, while a non-state actor's involvement in manipulating the cyber-space is termed cyber-terrorism. The ultimate objective of both the entities is almost the same, while the intentions may vary. Cyber-terrorism is an evolving concept with possibilities of critical damages to infrastructure, networks and cyberspace. Issues of cyber-terrorism are vital to information security specialists and to some extent the society. There are cyber armies all around the world: China having the biggest cyber-army in the world. The Unit 61398 of the Chinese cyber army is partially situated on Datong Road in Gaoqiaozhen. The US is also responding back equally with a lieutenant general appointed as the head of cyber-army in the US. The cyber mission force of the US is divided into four teams: the National Mission Team, which is responsible to defend the US and its interests against cyber-attacks of significant consequences; the Cyber Protection Team, which is responsible to defend Department of Defense networks and systems against priority threats; the combat mission team responsible to support combatant commands by integrated cyberspace effects in support of operational plans and contingency operations; and the support team, which is responsible to provide analytic and planning support to the national mission and combat mission teams.

In the cyber domain, there is a war going on between China and the US. The intentions of the Chinese were exposed due to their unsophistication as compared to Russians and Israelis cyber-armies. Currently, the Chinese intrusions into the US military or corporate sector have reduced raising many concerns. The two countries can possibly be indulged in a mutual agreement to make efforts to reduce cyber-attacks as a sign of 'seize fire'. It is also possible that the Chinese hackers have become more sophisticated, due to which the intrusions are going un-detected by the US system.

Cyber-Warrior

The speaker defined cyber-warriors as the best intellectual minds, studying in elite universities, with enormous knowledge into the cyber-space. These individuals need to be recognized and utilized through military and intelligence training, to help maneuver techniques to protect a country from cyber-threats. These intellectuals must have the ability to bear the stress of military training and intelligence operations.

Attracting cyber-geniuses from the universities is not impossible. If CIA consists of 50-60% of Ivy League graduates, then so can ISI. Various measures must be used to have such minds work for the cyber-security of Pakistan. If the efforts of harvesting cyber-warriors fail, the repercussions will be disastrous. Similar to the command-and-staff course for first-hand physical training, cyber-warriors can be exposed to multiple cyber-threat as part of a training program. This exercise will help them recognize, and thus fight cyber-attacks effectively.

Collaborative efforts under the following three dimensions will enable Pakistan to quantum leap in the cyber-space:

1. Human Resources: Prevent internal and external threats of data theft or manipulation
2. Network & Infrastructure: Develop sophisticated network infrastructure security solutions.
3. Hardware: Preserving the hardware, for software development

Conclusively, the speaker proposed the development of a Cyber-Warfare Academy to training individuals for the cyber-wars to come. Pakistan Cyber-Warfare Academy (PCA) can help train cyber warriors for national cyber defense and offense. The academy must work parallel to the naval academy, military academy and air-force academy, protecting

the interests of Pakistan from all dimensions. He also recommended that Pakistan's military and political leadership should initiate programs to identify country's critical infrastructures and vulnerabilities and help develop an organization such as Pakistan Cyber warfare Academy (PCA), training centers for cyber warriors for national cyber defense and offense. It will help to train them in both cyber security and military/ intelligence. Moreover, both public and private organizations need to work together to achieve the capability.

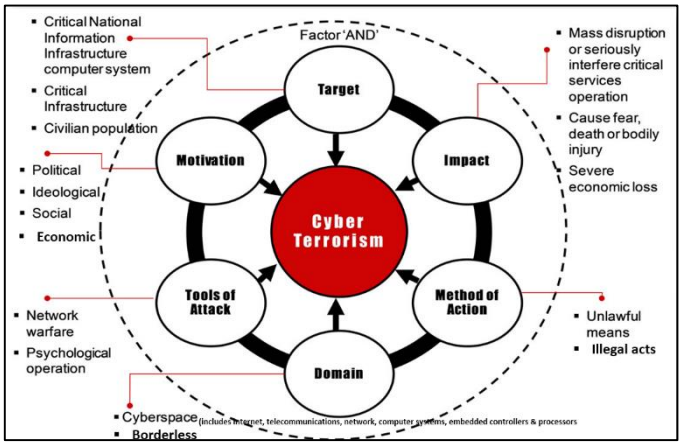
Speaker 2:

Mr. Irfan Ur Rehman

Former Head of Cyber Security Operations at PTCL

Cyber-terrorism at International and Domestic level

Mr. Irfan Ur Rehman commenced his speech by stating that the dimensions of terrorism have reformed. Terrorists today preferably use virtual weapons to damage the enemy rather than physical weapons.



Today, a single hacker can completely compromise the national security infrastructure to get the control of the internet, education, health, banking and electricity systems. With the rapid development of technology, cyber terrorism is also

increasing. Soon, a click on the keyboard will cause more collateral damage than a physical bomb. The United States of America has officially declared cyber-warfare as the fifth domain of warfare after land, sea, air and space. This should help Pakistan realize the grave importance of cyber-warfare.

Factors contributing to the aggravation of cyber-terrorism:

1. Lack of understanding of security risks in the cyber-space
2. Lack of funding to acquire adequate security tools and solutions
3. Lack of awareness regarding cyber-security in the general public
4. Usage of decentralized crypto-currency

Examples of cyber-terrorism:

1. Attack on Iran's nuclear facilities
2. The 9/11 twin towers attack also contained an element of cyber terrorism as the terrorists had carried out detailed research on the twin towers
3. The power cut in Ukraine through a compromised endpoint from the electricity department of Ukraine
4. A Lockheed Martin stealth aircraft manufactured in the US was hacked by a Chinese hacker.
5. The core routers of Pakistan are being compromised by CGSQ due to the inbuilt vulnerability of the Cisco IOS. It was hacked in 2006. The lack of centralized monitoring analysis system and forensics, compromise the information.
6. Mobilink CGR servers were hacked.
7. NADRA database was also hacked through the database application provided to the vendor.

Prevention of cyber-attacks:

He further stated that China has adopted the concept of 'Great Firewall of China'. China is using its own social media networks, messengers and search engines. Pakistan can develop a similar system linking networks, applications and search engines, to be in complete control of the information sharing.

Mobile operators can offer inbuilt social media applications and systems in smart phones, so the risk of a third party manipulation is eliminated.

National Cyber security strategy:

Defense strategies need to be focused upon, rather than offense strategies. Different malware and Trojans can obtain data or information from other countries, but the defensive side lacks infrastructure and sophistication.

National governance need to focus more on cyber-space running the risk, compliance and policy framework. Cyber-security policies need to be accommodated with governance and implementation.

He further proclaimed that the human resource needs to be harvested in an effective manner by providing them with incentives and opportunities to work for the country.

Pakistan's national response to the cyber-attacks needs to be strengthened. The centralized capabilities to counter and respond to cyber threats need to be improved by incorporating holistically integrated framework. Thorough consensus, coordination and cooperation needs to be developed to align institutional objectives regarding cyber-security.

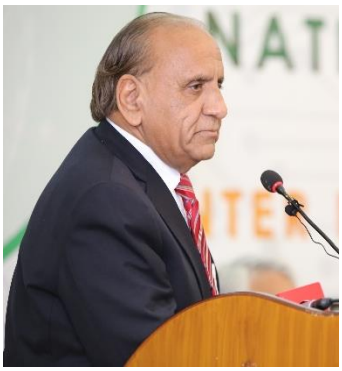
The speaker concluded his speech by manifesting the fact that the intangibility of cyber-threats should not be confused with lack of danger to national security.

Speaker 3:

Mr. Ammar Jaffery

Director General, Center of Information Technology (CIT)

Emerging New Technologies in Cyber Space



The speakers commenced his speech by enunciating that in today's world, the internet has become a basic necessity of a human being. There are three eras of the internet. The past, present and future. Internet of the past was used specifically for communication purposes. In the present, we are in the era of internet of things, responding to all forms of information within milliseconds. Internet of the future is the most worrisome for the users of today. A rough estimate claims that by the year 2020, 50 million devices will be simultaneously communicating with each other. The future is what the world today needs to prepare for. He further stated that the threats in the cyber-domain are exponentially increasing. There is thus a need for safety of critical infrastructures and building gaps between relevant stakeholders.

Today's terrorists are using the internet for the command and control systems for recruiting. The era of cyber criminals has been transformed into the era of cyber terrorists. Cyber criminals can inflict huge damage on infrastructure with almost no cost. The virtual world for criminals and terrorists is a real one. The influx of technology in individual lives cannot be stopped. In order to prevent cyber-crimes and attacks, understanding the technology before the criminals is necessary. No government in the world today can think of working without access to the internet and technology, due to which the traditional diplomacy is reshaping into e-diplomacy.

He further states that cyber-crimes pose grave threats to critical infrastructure. Pakistan requires strong mechanisms to counter such threats. Currently different public and private institutions are working in isolation from one another. A cyber-security policy must be formulated to integrate and synergize these individual entities into a single

collective effort to fight cyber-crimes. The country also needs to understand the difference between cyber-crime and cyber-security. Every individual is a victim of cyber-crime. There are existent laws for cyber-crimes, but they lack policies for cyber security.

He further stated that the future innovations in the world will be regarding crypto-currencies, internet of things (IOTs) and artificial intelligence. The democratization of artificial intelligence is excessively worrisome and will pose new challenges in cyber-space.

In today's rapidly changing environment, a behavior based approach is required to blend technology and human interaction. The criminals and terrorists are advanced, organized and smart. Thus, a corresponding system needs to build corresponding infrastructure, manpower, regulations and response systems. Pakistan also needs an incidence-centric report. The occurrence of an incident needs to be immediately analyzed and reported, to prevent similar occurrences in the future.

In the next two to three years, 95% of things will be in the cyber-clouds. Thus, understanding the ecosystem of the cloud holds crucial importance. In the cloud, things work in sync and are interdependent. If one element is damaged, it will disrupt the entire eco-system.

Elements of Cloud Services:

1. Hardware
2. Software
3. Integrators
4. Engineers
5. Third party vendors

The interdependence within the system is increasing quickly. Therefore, the dangers posed by a single point of failure are also simultaneously increasing. Software-as-a-service trends are catching up, which offer cheap solutions but are difficult to integrate.

Disaster recovery challenges:

The previously devised disaster recovery strategies are outdated today. They were most reactive strategies only utilized once a disaster struck had struck. Pakistan thus needs a proactive approach which will anticipate the threat before it materializes.

Opportunities:

The speaker further stated that the need to introduce cyber insurance for organizations is necessary. In three to five years, the banking systems will change greatly. Industrial revolution 4.0 will take over the world. Thus investments are needed in the SMEs, to make the system prone to the upcoming change in the cyber-environment.

The Way forward:

Concluding the speech, Mr. Ammar Jaffery talked about the need for an ecosystem comprising of the government, private sector, business corporations, academia, civil society and the public.

A cyber-security policy drafted in 2013 with the help of all stakeholders needs to be implemented. Pakistan also requires research and development to immediately identify new patterns of threat in the cyber-space. Cyber scouts and warriors need to be engaged effectively in countering cyber-crimes. Cyber drills must be conducted, both at national and international levels. There is also a need for regional & global cooperation in cyber-security. The capacity building of law enforcement authorities, with regards to cyber-

security need to be worked upon. Accumulative efforts can help strengthen the cyber-security of Pakistan against new threats and challenges.

Speaker 4:

Mr. Yusuf Hussain

Chairman IGNITE – National Technology Fund, Ministry of Information & Technology

Strategy to invest in Research and Development in Cyberspace

Mr. Yusuf Hussain commenced his speech by congratulating the organizers of the seminar. He further added that in today's world every individual is scared of cyber security threats. Exemplifying various threats he talked about the Iranian and Russian manipulation of the American election. Further on explaining the audience the significance of an innovation, he mentioned that when an idea is transformed into a product or service the impacts is observed by the entire society. The core question that arises from these challenges is 'are you going to buy a product from overseas or are you going to build a product yourself?' The former brings with it the threat of having a trap door or a security leak, while the latter requires innovation.

The speaker focused on innovations required for a self-built product and the time needed to develop such technologies. A threat that may not be imminent today, might become of concern a few years down the line, making current solutions obsolete. Thus, IGNITE works to make innovations that unlike a research project, solve problems pertaining to different sectors and professions of the society.

Artificial intelligence:

Artificial Intelligence currently helping doctors and lawyers abroad in researching databases to come up with referral cases, and judge profiles much better than a professional lawyer. In Shaukat Khanum Hospital Pakistan, a cancer diagnostic system is being developed to detect cancer, ten times better than a doctor. IGNITE itself is currently funding a diagnostic system for detecting bovine/cow diseases, which helps dairy production and elongates the cow's life.

Robotics

Robots around the world, are replacing jobs. A textile manufacturer in India has mentioned that robots will be taking away 10,000 jobs in the times to come. Letting robots replace humans, creates unemployment, but not doing so leads to lack of competiveness, decreasing exports even further. Pakistan is currently working on various innovation projects such as a fire-fighting robot being created in Karachi. He further proclaimed that with time the threat multiplies, as it is not just one device but all devices that are endangered by cyber-attacks. The behavior patterns of individuals are analyzed by Google and Facebook, finding out what they would want to buy and when, and so the pop-ups come up as per the prediction. This is called analyzing data, to create a personality profile.

Block-Chain

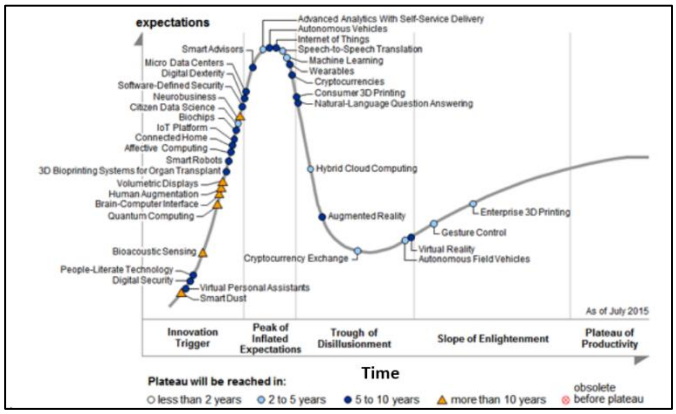
A block-chain is a system through which any individual can run an IT system without the assistance of another system. A block-chain creates similar opportunities without requiring a central authority. Currently, the block-chain is being utilized for crypto-

currency such as the bitcoins. The block-chain facilitates transactions that cannot be tracked using the dark web.

Neuro-tech

Neuro-tech is a developing technology that can read an individual's dream and mind. It can also place a training module in your brain. Some of these technologies are still in the process of developing, but they will be seen being utilized in the near future. He further stated that no cryptography can sustain quantum computing.

The world economic forum has stated that cyber-security can no longer be seen as a primitive defense, and should rather be seen as cyber resilience, assuming that the parameter will be breached. Once the parameter is violated, the response mechanism needs to be worked upon.



Everything being discussed today is not happening immediately, but the pace of development in the cyber-world is worrisome. Thus, the speaker proclaimed, that unless an extensive strategy is devised, incorporating a policy framework, technology, innovation and training, protection against cyber-threats will not be possible.

Elements of cyber-security:

1. Network
2. Application
3. Data
4. Host

IGNITE mostly deals with developing technologies for network and application. IGNITE is currently building a Pakistan-based artificial intelligence matching employment software, to preserve the data. Data access and possession holds a lot of importance in today's world.

Projects by IGNITE:

Machine Learning, Artificial Intelligence (Developed Aug 2008 - July 2011)

- The project developed scalable security-based packet marking methods, including security-induced packet marking at wire-speeds within the core network.
- It also developed robust strategies for discarding of security-marked malicious packets and ensured stability, fairness and convergence objectives for benign and legitimate flows.
- Pakistan Education Research Network (PERN) significantly benefitted from the network-embedded security framework.

A company called Plum-Grid was made around the project, which was then bought by an American software company called vm-ware, turning out to be a great success.

Machine Learning, Artificial Intelligence (in progress)

N-Visible is a network application that performs real time analysis for anomaly detection, compliance, profiling and reporting, with minimum human intervention, using cognitive visualizations and machine learning.

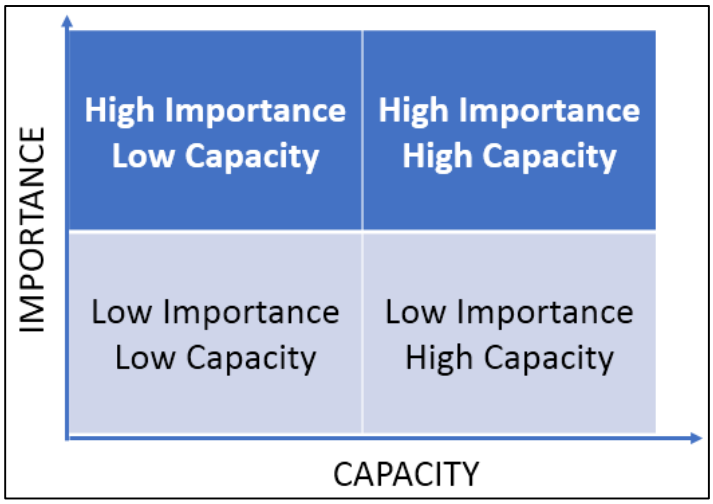
Signal Processing, Wireless Communications, Embedded Systems, Defense/Tactical Communications (in progress)

- Lead the world to next-generation tactical communication SDR waveforms based on the 5G Technology
- To employ the dual-use SDR technology for bridging the gap between commercial and defense industry
- To tap the huge tactical communication market in Pakistan and other regional countries
- To help academia and research organizations in Pakistan by creating a skilled human resource pool and putting stop to brain-drain

RFID, Micro controller (Developed July 2013 – December 2014)

The speaker further stated that iFahja has developed a solution that overcomes the issue of existing RFID based security systems by using a password to authenticate the user. Stolen car, a stolen e-tag, a regenerated e-tag would not be used to enter the secure premises.

Coming up with an R&D Strategy requires prioritization



A detailed strategy is yet to be devised, but prioritization for devising a strategy can be done on the basis of the graph. Network, application, data and host can be used to build systems, which can deflect different kinds of threats. Some products can be produced locally, while the rest can be brought to the international market, to meet the requirements of the strategy. Such a strategy is hard to develop within the government or the military. Around 15 years ago, the US tried to build a secure database, spending $60 billion on a failed database. The failure was caused by the small span of product lifecycle, constantly requiring innovation. Consequently, there will be undeniable challenges along strategy building.

Build organizational drivers around Startups

Innovation is always built by startup businesses. Today, the 5 most valuable companies of the world, were once like any other startup. All these startups, are bringing in industry, academic, government research, bringing it together and generating results. The following is a list of startups operating within and beyond Pakistan:

Government

- Defense Organizations safe guard against cyber threats
- National Telecom and Information Technology Security Board (NTISB)

- MoITT Cyber-Governance Policy Committee

Startups and Industry

- Trillium
- Five Rivers Technologies
- Security Wall
- Cyphlon
- Ciklum Pakistan
- PISA
- C@RE

Higher Educational Institutes

- Military College of Signals
- Riphah University
- Lahore Garrison University
- Air University

Global level

- Sparkcognition
- Elastica
- FireEye

All three of the top, global level cyber-security companies were either built by a Pakistan national, or a Pak-American national. This means that Pakistan does not lack the brains, and with the rightly invested potential, a cyber-secure Pakistan can be created.

Speaker 5:

Mr. Tariq Malik

Former Chief Technology Officer, GHQ

Internet of Things (IoT) – A Case Study from security prospective

The speaker presented a middle eastern country's smart city case study related to Internet of Things (IoT). The ruler of the city decided to make the city a happier place to live. To achieve the objective, they must measure citizens happiness level with the government provided services. They created a smart city department with a clear mandate to make the city happier place and use technology to achieve measure and improve it. Internet of Things (IoT) based sensors are sending quality of service data for onward analysis and performance measurement of the services. The collected data is also used for improvement and planning of future services. This collection of data and further dissemination must be securely executed.

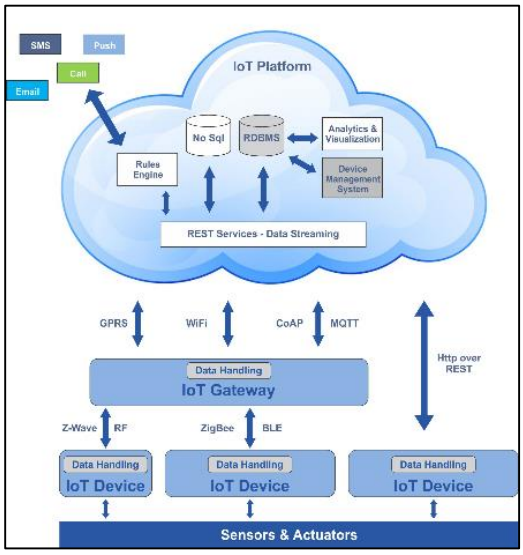
To secure such a complex environment the speaker further explained that the city has several departments and each department has thousands of sensors spread across the city collecting data. Each department then sends the data to smart government data center. The data is carried back via telecom operator. There exists a large cloud infrastructure, along with an application provider and integrator. Backend application with data repository, its security and managing the authenticity of sensors, communication and encryption is known as 'IoT platform'. The platform is what manages all incoming information. The problem is, sensors are unintelligent devices, and are installed in millions. A culprit can change the firmware of a sensor and may use it for cyber-attack against the city. A sensor could be easily manipulated in re-channeling the information, incorrect data or causing delays. All these cases can create issues for city managers and

may damage their services, including damage to important services such as trains and aviation traffic.

Project Background (Multiple Players)

Project complexity included

- Department owning the Sensor / Data
- Smart Government
- Telecom Operator
- Cloud Infrastructure
- Application Provider and Integrator (Platform)



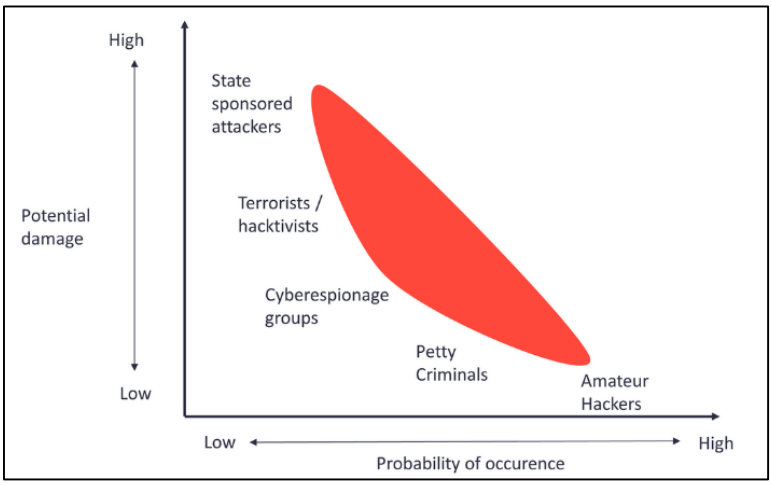
There are 3 different components of an IoT model, namely the platforms, gateways with several different communication mechanisms and the devices. Sensors can be from the range of 5 cents to 40,000 dollars per sensor, depending upon its life-span and placement.

The problem arises with the device owned by a single organization e.g. Electricity and Water Authority (EWA). Which has automated meters for gas and electricity, the meter, must communicate back meter readings. A hacked meter's data can be rerouted or corrupted with the possibility of stealing electricity. EWA alone has access to this sensor. But the data might be required by the government, for which there needs to be a mechanism through which data with one organization can be viewed by multiple organizations. In such a case, Data or Metadata must be made available to multiple organizations. This is an extremely complex structure, each having a domain of their own and keeping data level security become challenging.

To secure the platform protocols to be looked upon:

- Infrastructure

- Identification– If the firmware of a sensor is changed, one can identify that the sensor now has a different code
- Communication / Transport
- Discovery: one cannot register millions of sensors manually, thus a system is required
- Data Protocols
- Device Management
- Semantic Multi-layer Frameworks
- Security (Open Trust Protocol (TEE), X.509) – most important, stores the cryptography to look after all the devices, while each device is given a certificate, which can be changed when required
- Industry Vertical (Connected Home, Industrial, etc)



Note: State sponsored attackers are of most concern in risk identification.

Security Challenges:

- Availability: Every time a sensor connects to a network, its firmware, the communication, certificate must be verified, encrypted communication needs to be started. If it disconnects and connects again, there is a cost because a disconnection indicates that something is wrong.

- Identity: Authenticating endpoints, services, and the customer or end-user operating the endpoint
- Privacy: Controls the access to the multi-tenant environment, reducing the potential for harm to individual end-users
- Security: Ensuring that system integrity can be verified, tracked, and monitored

For example to connect millions of sensors together a neighborhood network (NAN) was created, and the network itself decides the meter to send back data.

He further stated that applications like the firewall are basic need but does not provide full security. They are not the solution to advance security threats. Security must be implemented at all the aforementioned layers, or else a secure environment cannot be ensured.

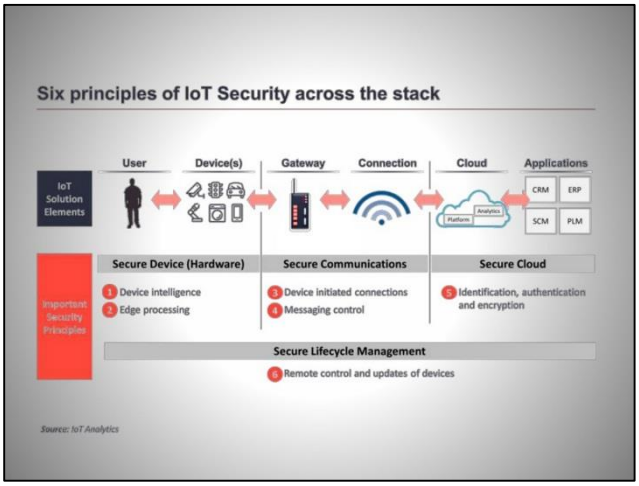
Requirements

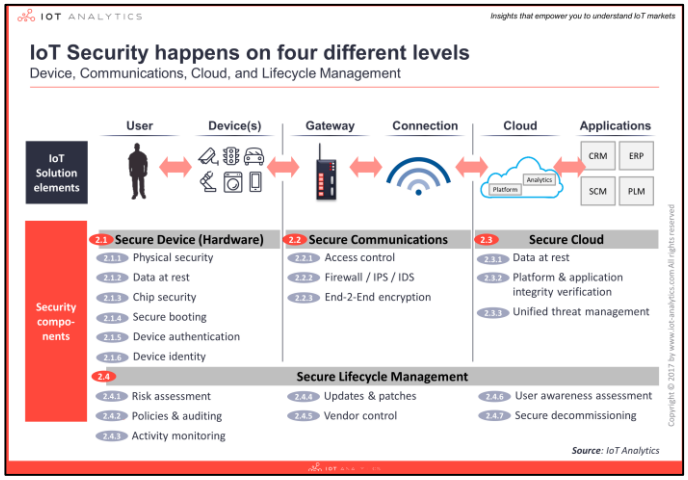
- The IoT platform should support Perfect Forward Secrecy (PFS)
- The IoT solution should support the remote disabling of certain features from a family of devices or the isolation of vulnerable IoT devices, as per a detected threat
- The Platform should provide mechanisms to detect malicious and anomalous activity or integrate easily into device side malware protection or anomaly detection products
- IoT devices should be able to detect and resist attacks from the edge including spoofing, replay, and excessive communications

Matrix

- Area (app, device, protocol)
- Risk (to itself and other tiers)
- Solution (development, wrapper, standard)
- Responsibility

- Timeframe





Trusted Computing Base

A trusted computing base was developed by a provider to detect anomalies.

Software Defined Perimeter (Black Cloud)

The concept was created by Defense Information Systems Agency (DISA). In this model software components communicate on a need-to-know model, in which device posture and identity are verified before access to application infrastructure is granted.

By implementing DISA, the most common network-based attacks, including following were mitigated:

- server scanning, denial of service, SQL injection,
- operating system and application vulnerability exploits, man-in-the-middle,
- cross-site scripting (XSS), cross-site request forgery (CSRF), pass-the-hash, pass-the-ticket, and other attacks by unauthorized users

Conclusion

Security of smart city project was extremely complex, but was achieved. Security was added at all the layers of IoT environment, from edge sensor to Datacenter, from

application to multiple department's users, from sensor registration to Platform and from data availability to data intelligence access.

Mr. Tariq expressed his views regarding general IT and communication security. He said, that an end user does not have to be an expert on IT security, they should the risk but shall not be responsible for security of their devices. It's the responsibility of IT providers to encapsulate complexity and take the security responsibility of their users. Security must be implemented at design stage, then the environment can sustain user mistakes. A user should only have applications necessary to perform their job, and nothing extra to make them vulnerable. The solution is to keep the complexity away from the user, and to be moved to data center.

Speaker 6:

Mr. Mudassar Hussain

Member Telecom, Ministry of Information Technology, Government of Pakistan

Attempting a Cyber Secure Pakistan

Mr. Mudassar commenced his speech by thanking the forum for letting him represent the Ministry of Information Technology. While discussing the challenges Pakistan faces regarding cyber security, he mentioned that a versatile audience globally faces similar challenges. For instance, in today's world, a two year old is aware of the consequences of cyber hacking, and so is the President of the United States. Given the commonality of interest, a state must first develop its own cyber security network, and then integrate it internationally, utilizing the global internet.

He explained the practicality of a 'stakeholder agreed consensus on a cyber-security policy', and talked about the importance of having a mutual consensus on curbing the challenges of cyber-security. A policy is not just a paper if applied consistently in alliance with institutional and regulatory structure. Only with mutual consensus can a cyber-secure Pakistan becomes a reality. Today, national security is not just military security, but also cyber, human and food security. Hence, contemporary responses need to be worked upon, to address the unfamiliar challenges the world faces today.

He further elaborated that while we construct an extensive cyber-security framework for Pakistan, we must ensure that none of the actions impedes the economic growth of certain sectors or limits the business options for the natives of the country. The stakeholders of a cyber-secure Pakistan, be it industrialists or the military etc., must have a mutual consensus on Pakistan's cyber-security policy with an overall governance structure and an institutional mechanism. The problem of the matter, however, lies in the actual policy formulated. The policy must cater to the needs of all stakeholders, and be in accordance

with the governance, institutional and cross-sector collaboration models. Currently, due to lack of collaboration between different sectors, a holistic image of our cyber-readiness has not evolved. He suggested that the policy should also present a risk assurance framework to address the ambiguity regarding the sources of the information received by users.

A self-created cyber-security framework may look like an attractive option, but the reality is much different. Even if such a framework is backed by research and development facilities of Ignite (formerly National ICT R&D fund), addressing the cyber-security challenges in isolation is not the solution. We need a policy that addresses the concerns of all local sectors, and that also acquires international collaboration.

The speaker also pointed out that the common user of the internet is widely uninformed about the threats cyber-crimes pose. The cyber-security framework must increase the awareness among individuals for the sake of protecting their own interests. While a rough structure for such a policy already exists, a revamped cyber-security policy should address all the mentioned concerns, and amalgamate them into becoming legislation for implementation. A cyber-security policy for Pakistan is the need of the hour because cyber-crime is no more a neglected threat but a reality. The successful implementation of such a policy however, depends upon the collaborative efforts made by different sectors in pursuing cyber-security goals.

Mr. Mudassar further on suggested a centralized system, to which second-tier sectors of banking, telecom; financing and energy will be attached. Such a mechanism will address sector-specific concerns, as well as keep all the sectors integrated with one another through the regulator.

Lastly, Mr. Mudassar mentioned that open and closed discussions are the key to developing an extensive cyber-security policy for Pakistan, and so quickening the process of developing such a policy is exactly what Pakistan needs.

Question and Answer Session

Moderator

Mr. Amer Hashmi – Advisor, National University of Science and Technology (NUST), Islamabad

Mr. Raza Khan

Question No.1

Are we prepared for facing a cyber-attack by countries by India or Israel? Countries like North Korea has a cyber-warriors team. Where do we stand with regard to cyber protection? Is there one single body only dealing with the issues of cyber threats?

Answered by Mr. Tariq Malik

People in Pakistan previously did not consider cyber-threats as viable threats, due to which Pakistan itself was lagging behind in developing Information Technology. Once, the severity of such a threat was realized, certain decisions were sped-up to curb the problem. The current cyber-security framework that has been developed, which the speaker himself reviewed in 2013, is considered proficient and workable, and so the implementations of the framework will be channeled accordingly. Pakistan requires a nominated body to integrate various sectors together, to deal with the menace of cyber-attacks. Unless all department work in close collaboration, the threats of cyber-space will exist.

Mr. Muhammad Iqbal

Question No.2

When Pakistan does have a cyber-security policy? Is the implementation of the policy problematic due to certain geostrategic challenges?

Answer by Mr. Ammar Jaffery

Putting geostrategic influence aside, Pakistan internally needs to appoint a focal authority, give it a timeline of three to six months to devise a plan. A document should be generated, put together the respective authorities, and place penalties when needed. The re-invention of the wheel is unnecessary. Thousands of documents are available on the internet that can help develop a more sophisticated implementation mechanism.

Comments by the moderator

The implementation of a cyber-secure policy is not entirely under the influence of geo-strategic players, but rather under a national authority, such as the National Security Division, thus the implementation is not sufficiently affected by geostrategic challenges.

Ms. Asna Hassan from Center for Global & Strategic Studies

Question No.3

While developing a cyber-security policy for Pakistan, what do you think we can do about the collection and manipulation of 'big data' by countries like the United States of America?

Answer by Mr. Mudassar Hussain

In the last few decades, the internet has evolved immensely. Some believe that the evolution was organic, while others believe that the deliberate efforts brought about the evolution of the internet. Today in all parts of the world, the personal data of individuals using online websites, is being harvested. The concern regarding the usage of this data is common to all involved. For any research or innovation, data is indeed the 'key'. The

question is 'how this data will be exposed by organizations like NADRA, and once exposed, will it be anonymous, to not compromise the privacy of the individual or organization.'

One way of working is to have a data protection law, based on international norms. Once a big bulk of data is collected, the countries can interact among themselves. This is a difficult process of having a correlation between nations. Even in the international community, there is still a lot of ambiguity about as to how will this data will be pursued by countries.

Answered by Mr. Yusuf Hussain

There are three different approaches to secure the data of a country. The first is the China approach, China has built a cyber-great wall, having their own search engines and interactive websites, isolated from the influence of the rest of the world. The second is a regional approach, the one European Union utilizes, through which each country in a region could protect themselves, a global consensus is unnecessary. And the third is a block-chain approach through with the block-chain developers enables individuals in protecting their own identity. It is easy to say, that Facebook is using individual data, but in return, Facebook is also free of any cost. Through a block-chain, individuals can decide which data to give out, and which to protect. Such a system gives you power as well as independence.

Comments by the moderator

Pakistan needs to develop data safeguards, which will protect the data of individuals from being manipulated. Currently, there are countries that have made massive success in securing themselves in the cyber-space, while others are still exploring the dimensions of the cyber-world. Pakistan for one is at the elementary stage, and so it has a long way to go in achieving cyber-security.

Wing Commander Mujeeb

Question No.4

What are the diplomatic efforts of Pakistan in formulating international legislation for cyber-security and what alliances is Pakistan making with like-minded countries with regard to cyber-security?

Answer by Lieutenant General Nasser Khan Janjua

Legislation on cyber-security worldwide, have to be common to all. Leading countries have a higher level of participation in documenting international cyber-security legislation, while all others can play their due part my expressing their expectations. The policies formulated under the umbrella of the UN take some time in evolving. Meanwhile, Pakistan plans on making its effective participation in making such a policy to guard Pakistan's national interests.

Pakistan has a long way to go, in developing alliances with regard to cyber-security. We need to identify the allies, which will negotiate terms with us as per the current state of affairs. Countries with similar interests can turn out to be better allies. However, cyber-security alliances are tricky. Many precautions need to be looked into to cater all the global dimensions of the cyber-space, and that is exactly what Pakistan is currently working upon.

Mr. Muhammad Osman from NUST

Question No.6

If all relevant challenges and solutions have been realized by Pakistan, then why do we lack in implementing these policies?

Answer by Mr. Mudassar Hussain

The challenges and solution in the cyber-space can be vastly, but not entirely explored. By far, Pakistan has had a policy for open information and open internet. For Pakistan to move towards isolating from the cyber-system, requires a major policy shift in itself. First, you declare yourself as a closed internet society. It is not a

matter of funding the shift, but a matter of whether we want to switch the course or not. A shift will have its own repercussions. By far, the discussion is focused on keeping the information open to the general public and our industries. All countries, even the US, face challenges in pursuing policies on cyber-security. In the US, hundreds of companies are pursuing cyber-security in their own specific domains.

Pakistan needs a collaboration mechanism. No single legislation has been so thoroughly discussed as the cyber security bill of Pakistan. It was debated upon by the civil society, as well as the government. The issue of privacy protection is common to all. But the implementation of such policies, along with keeping the free and safe, is a value-adding process.

Answered by Mr. Tariq Malik

Organizations like the European Union and its defense mechanisms are very different. Pakistan is still devising its priorities as per the needs of the cyber-environment to implement policies. He further stated that China is open, it is not blocked. China has just created their own applications. Sharing his own experience, he talked about conveniently communicating with Chinese counter-parts and friends on we-chat. Individuals can go buy things from Ali Baba. China is, however, managing and controlling its own internet. The issue Pakistan faces is regarding the financing. Once sufficiently funded, telecom operators and providers need to be trained, to secure the network, while also letting it be open.

Ms. Maria Khan

Question No.7

How can we secure our cyber data from social media websites?

Answer by Dr. Muddassar Farooq

Encryption and encryption protocols can be applied to secure the data. End-point security is always highly crucial, because that is where the attack

occurs to steal the data. End-point security is thus primitive. Thus the solution is to use standard encryption and harden the entry point security accordingly.

Answered by Mr. Mudassar Hussain

The way these companies have come up, they are products of innovation, once companies like Facebook and Google became corporate citizens, they also became corporate citizens to the US system and followed their laws. Having access to data requires mutual legal assistance among companies. Treaties under the UN to seek information have been negotiated in accordance with the data available. Companies can now sense the curiosity the individuals have towards these applications. Pakistan, thus, requires strong implementation of data protection laws that will define the usage and repercussions of intermediaries using your data.

Comments by the moderator

The policy regarding cyber-security exist, but the lack of implementation is due to the lack of training provided for research and development professionals.

Mr. Muhammad Ali

Question No.8

Donald Trump's new nuclear posture, according to the New York Times, stated that the United States is considering lowering down its nuclear threshold; a cyber-attack may be responded through a tactical nuclear weapon:

a. Is this true?
b. Are we (as Pakistan), in accordance with other nations, considering lowering down our threshold, to respond to a cyber-attack, with a tactical nuclear weapon?

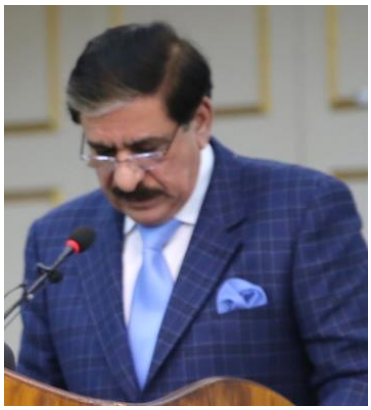
Answer by Lieutenant General Nasser Khan Janjua

Lowering of the threshold is an independent stance of a country, addressing defense concerns. The Trump government has paid a lot of emphasis on enriching the American Nuclear Arsenal. The United States lowering the threshold, against cyber-threats should make us realize the importance the Americans give, to the issues of cyber-security.

Individuals mix up Pakistan's defensive views with that of the United States. The nuclear narrative of Pakistan is well thought out, and has no linkages to the direct changes. the US may be making to its policies. He concluded his answer by stating that America's strategy may not be Pakistan-centric, but for the entire globe, so a direct correlation should not be made between the two entities.

Closing Address by

Lieutenant General Nasser Khan Janjua, HI (M), (Retd) – National Security Advisor, PM Secretariat, Islamabad



General Janjua commenced his closing address by congratulating Center of Global & Strategic Studies and National Security Division on collaboratively organizing a befitting seminar. He further expressed his reverence towards the addressed cyber-security concerns and questions, and assured the audience that all will be incorporated into a framework.

The growing digitalization and amalgamation of cyber-space in defense and security, have caused the emergence of new threats. The entire sphere of the cyber-space is monopolized by the one with the correct knowledge. It is thus the responsibility of each consumer to transcend the knowledge of the cyber domain, to learn about the ones who monopolize the domain, then become the same. He believed this being the solution to the cyber-security concerns.

Further to it, he mentioned that Pakistan is deeply engulfed in addressing its traditional and conventional threats, that the country neglects the threats emulating from non-conventional innovations. Without any further ado, existing and new threats need to be confronted simultaneously. We as a nation, need to effectively address the rising challenges, now more than ever before.

Cyber-threats happen to be a fairly new challenge to many nations. Many of such nations are still in a process of developing a cyber-security framework, to protect its national interests against the threats posed by the cyber-space. Information technology in today's date profoundly affects the thought process of a state, with regards to warfare and security. The advancement in technologies has created many seen and unseen boundaries which transcend the influence of states. With increased dependence on digital technology, rises the need to secure our information from being maliciously disrupted or misused. On one hand, the internet provides us with information, and on the other is poses a security threat to the state. The need of the hour is to develop cyber-security solutions to protect

information, along with benefitting from the World Wide Web. With the growing sophistication of cyber-attacks, programmers have been unable to entirely protect computers, data-bases, programs and networks. Pakistan being a country with strategic capability, currently needs to securitize its cyber-space to protect communication systems, financial systems and conventional systems against cyber-threats. At a societal level, Pakistan's cyber-security is highly vulnerable to threats. This increases the chances of losing critical information and disrupt national critical infrastructure of the country. Enemies can exploit, disrupt and destroy information to harm the state. Cyber-security should not just be addressed as per priority for the government, but also should be prioritized by individuals, as a direct national threat. Currently, only a few individuals understand the gravity of the issue.

Furthermore, he mentioned that Pakistan must utilize the already established E-governance council, to formulate a policy with inter agency coordination and an enabled environment, to research and enhance the capability of various branches of government, academia, information and security profession. The policy must also cultivate awareness among individuals about the severity of cyber-security.

General Janjua concluded his remarks by stating the importance of a collaborative effort of individuals, organizations, companies and institutions to take responsibility to protect their respective parts of the system to create a cyber-secure Pakistan. The advisor further mentioned that the digital regime stretches around the globe, irrespective of geographical boundaries. The core objective is to align Pakistan's standards of cyber precautions, preventions and preparations with international standards. Lastly, he called upon experts to extend a helping hand and requested the state institutions, corporate sector and the general public to effectively leverage potential in this field.

Concluding Remarks by

Lieutenant General Muhammad Zahir Ul Islam HI (M), Retd – Chairman CGSS

The Chairman initiated his closing remarks by expressing his gratitude to all those that added to the success of the event through active participation. He extended a special thanks to General Nasser Khan Janjua for providing Center for Global & Strategic Studies the opportunity to be a partner in this important conference. He further stated that the level of expertise demonstrated at the seminar had humbled me immensely.

He shared his experience from a War College in the US, which had many international students. Scandinavian countries have achieved a lot in regards to cyber-security. Moreover, he mentioned a Swedish army officer, who narrated extensive progress his country had made in cyber-warfare and cyber-security. They had designed a strategy, a game was designed. The game comprised of two teams. The red team comprised of hackers, who attacked the cyber-security networks of the other team. After an ongoing effort of almost three years, a complete cyber-security network was created. To test the security network, hackers from around the countries tried to break through the system. The individual who ultimately broke the code in a week's span was a young whiz kid from Pakistan.

He concluded his remarks by stating that Pakistan has the potential. The intelligent individuals of Pakistan should be able to provide the required cyber-security. To sum up, he extended his faith in the cyber-security team led by Lieutenant General Nasser Khan Janjua in devising a 'Cyber-Security Policy' addressing all concerns discussed at the seminar.

Recommendations

National Cyber Security strategy is an essential component of any country's Overall Security & Development Strategy. The responsibility includes protection of its citizens, assets and information against cyber terrorism and implementation of measures to help achieve this responsibility.

It is challenging but possible to catch up with the increase in national cyber threats and counter it with appropriate vigilance and response from the government. National Security Division has rightly tried to highlight the issue for all stakeholders. There is good understanding of the issue within the higher echelons. Moving onwards, this understanding is now required to be transformed into concrete steps towards formulation of a national strategy and its responsibility matrix.

For proper execution, the cyber security response and its control responsibility must lie with an empowered Organisation properly mandated for this purpose by the government. This body must be allowed to act as a steering committee to coordinate the plans and efforts of different departments on agreed milestones, while ensuring their culmination into a cohesive National Cyber Security Framework. The LEAs, armed forces, FIA and civilian organisations may be encouraged to continue to perform their individual roles within the overall ambit of this framework. It is to be ensured that each of the efforts feeds into the achievement of specific objectives of the strategy.

National mandate is missing from the equation with multiple stakeholders and unclear jurisdiction. National level role and effort at federal government level to glue fragmented efforts and to device the national cyber strategy is missing.

The learned panel highlighted several cyber security related issues and recommended methods to close the gap. They also emphasized the need of:

- A national body to lead the space
- Creation of human capacity building
- The threats within the cyber space
- Funding available for research and development
- Case studies of neighboring countries, and
- Cyber security awareness and work required.

Based on the discussions and input it is recommended to:

- Mandate the creation of a group under National Security Division to discuss and recommend national level security strategy and a framework to achieve its objectives. The group to consider following while preparing their recommendations:
  - Creation of National Cyber Security Organization (NCSO). Define their mandate, coverage, responsibility and authority.
  - Brainstorm and identify priority areas for the NCSO to focus on
  - Creation of National CERT (Computer Emergency Response Team). Define their mandate, responsibility and finances required.
  - Define pillars of our cyber security strategy and a framework on how to take them along
  - Cyber security Centres where local research and development shall be encouraged by:
    - Local Universities to develop intellectual property and capacity building for equipped manpower
    - Funding by Government (IGNITE)
    - Indigenous security products to be developed and supported by Government.
  - Create a program to review and update the existing policies at departmental and division level to harmonize them in line with the framework
  - Security awareness campaign for Government and Citizens

Center for Global & Strategic Studies
Islamabad

National Security Division, Government of Pakistan

3rd Floor, 1-E, Ali Plaza, Jinnah Avenue, Islamabad, Pakistan

Tel: +92-51-8319682

E-mail: info@cgss.com.pk Website: www.cgss.com.pk