Cyber Space Security in South Asia

Compiled by: Haris Bilal Malik
Reviewed and Edited by Khawaja Dawood Tariq

STRATEGIC VISION INSTITUTE (SVI), ISLAMABAD

Strategic Vision Institute (SVI) organized a webinar on “Cyberspace Security in South Asia” on 28th January 2021. The webinar was chaired by Dr. Zafar Iqbal Cheema (President/ Executive Director, SVI). The speakers included Mr. Khawaj Dawood Tariq (Senior Research Associate, SVI), Dr. Nasir Mehmood (Assistant Professor, Strategic Studies, NDU Islamabad), AVM (R) Faaiz Amir (Member/Educational Consultant, Higher Education Commission Pakistan), and Dr. Tughral Yamin (Associate Dean, CIPS, NUST Islamabad).

The webinar deliberated upon how cyber space has evolved into the new domain of warfare in the 21st century. South Asia too had been affected by this emergent warfare domain because of Indian aspiration to dominate cyberspace. Pakistan appears as among the most spied countries and was also among the most vulnerable countries as far as cyber-security was concerned. The impact of cyber and information operations on the security of the region is being exacerbated by the inter-state conflicts. India had significantly enhanced its cyber capabilities and was seeking to dominate regional cyberspace. Indian IT industry’s figures for the last fiscal year and generated revenue of $191 billion, which made over 8pc of India’s GDP. Growth of the IT sector at such a huge pace, moreover, helped India greatly off-set its import bill. India is likely to introduce a new cyber security policy this year. States compete for superiority at the local system level to impact other countries at psychological and decision-making levels by causing major disruptions and occasional damage. India had a large technical force to be a factor in a conflict. Although security ranks high on Pakistan’s national agenda, in the increasingly complex threat milieu, cyber security usually got relegated to the bottom rung and sometimes was ignored. Therefore, Pakistan is way behind other countries in protecting itself in cyber space. In this regard, effective policies and legislation are needed to counter the ill-effects of debilitating cyber-attacks. Furthermore, the intensification of India’s cyber-attacks against Pakistan requires enhancing cyber capabilities by the latter.

After offering a warm welcome to the participants and webinar audience, Dr. Zafar Iqbal Cheema explained in his opening remarks that Cyber space is the new domain of conflicts in the 21st century. Since the advent of technological innovations in warfare, ‘Cyberspace’ has considerably emerged as the new battlefield for states. The South Asian region has also been impacted by this complex warfare domain. This is primarily because India aspires to dominate the regional domain of cyberspace. The international and western literature suggests that Pakistan is among the most spied countries. It is also among the most vulnerable countries concerning cyber-security. In the wake of India’s offensive policies towards Pakistan in which, along with others, cyber security holds great significance. In recent years, there has been an intensification of India’s cyber-attacks against Pakistan. India has a larger cyber operations capability as compared to Pakistan. India has carried out various operations against Pakistan whereas; the latter has not carried out as many cyber operations as the former does. The growing complexities of cyberspace and the acquisition of offensive cyber capabilities by India have threatened Pakistan’s cyber security. In South Asia, cyberspace has become an emerging warfare domain which India aspires to dominate. He further added that given the rapid expansion of cyberspace at the regional level, cyber-attacks have become more lethal as these pose a serious threat to the national security of Pakistan. To cope up with such cyber threats posed by India, Pakistan needs to further enhance its cyber capabilities. He said, keeping these points in mind, it would be interesting to see how this discussion will proceed.

Dr. Zafar Iqbal Cheema invited **Mr. Khawaja Dawood Tariq** to present a short primer on “Cyber Space Security in South Asia”. He started his primer with a famous quote;

“The supreme art of war is to subdue the enemy without fighting” Sun Tzu.

Every new technology presents the possibility of new weapons, and for every new weapon, there’s a soldier hoping it will yield the ultimate advantage, although few ever do. Much has been dedicated to the power of navies and air forces to change the face of warfare. Nuclear weapons have further complicated the picture, creating a top tier power overshadowing the conventional conflict. Today’s net-centric world proffers a new weapon. To many, cyber-warfare represents the 5th battle-space—a new type of warfare in need of further definition. To others, it is merely a new weapon to be integrated into traditional conflict.

In the age of code wars, have our lives changed for the better? Are we any safer than the bloody wars or the cold wars from the past? Are there any more guarantees now in a cyber-age than in a kinetic age involving human conflict? These are the types of questions that have few answers due to the secret nature of the operation. However, its importance cannot be denied. In 2017, Russian President Putin declared that “Whoever becomes the leader in [artificial intelligence] will become the ruler of the world.” In May 2018, Chinese President Xi Jinping told the Chinese Academies of Sciences and Engineering of his plan to make China “a world leader in science and technology,” which includes “integration of the internet, big data, and artificial intelligence with the real economy.”

Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks. The distinction between exploiting weaknesses to gather information – also known as “intelligence preparation of the battlefield” – and using those vulnerabilities to do damage is impossibly thin and depends on the intent of the people doing it. Intentions are notoriously difficult to figure out. In global cyberspace, they may change depending on world events and international relations. The dangers – to the people of the countries both allied and opposed – underscore the importance of international agreement on what constitutes an act of war in cyberspace and the need for clear rules of engagement.

The vulnerability of digital networks is, in many ways, an inevitable consequence of how the Internet was built. As then-Deputy Secretary of Defense William Lynn put it in a 2011 speech announcing our military strategy for operating in cyberspace: “The Internet was designed to be open, transparent and interoperable. Security and identity management were secondary objectives in system design. This lower emphasis on security in the internet's initial design … gives attackers a built-in advantage."

Among many factors, two, in particular, contribute to the growing sense of unease. One is the problem of anonymity. Those who seek to harm can easily do so at a distance, cloaked in the veil of anonymity behind false or shielded identities in the vastness of the web. With no built-in identity verification, pretending to be someone else is as easy as getting a new email address or registering a pseudonymous Facebook account. Second, and perhaps more significantly, the online world changes the boundaries of war. Unlike standard weapons of destruction, cyber warfare is harder to trace as elements like malware can be embedded into a system secretly. Often, state-sponsored attacks go unclaimed, leaving room for speculation. Then there are the occasions when hacking groups admit their crimes, but the problem is that they're never "officially" liked to a particular state.

Referring to Cyberspace security in South Asia he deliberated that the India-Pakistan conflict seems to have found a new battleground. The threat of Indian cyber-attacks against Pakistan becomes more serious given India's growing investment in advancing its cyber security expertise. Indian space endeavors are primarily focused on commercial activities such as spatial navigation. However, there are multiple reasons as to why the Indian Space Program is a matter of concern for Pakistan's security interests. In recent years, India has stepped up efforts to strengthen its defensive and offensive cyber warfare capabilities. Due to its rivalry with Pakistan, both countries could potentially target the other with cyber-attacks. Although neither Pakistan nor India has carried out a large-scale cyber-attack against each other so far, small-scale cyber-attacks between both neighbors are becoming frequent. Web vandalism especially is very common.

In 2019, the mobile phones of some senior Pakistani officials were hacked for covert surveillance. The hacking was done via WhatsApp using a special type of malware called "Pegasus," allegedly developed by Israeli spyware company the NSO Group. The malware could infiltrate a phone by making a missed call on the targeted WhatsApp number and turn on the phone’s camera and microphone as well as gain access to messages, emails, contacts, and passwords. The malware also has the capability of determining GPS location.

Indian policymakers are now also looking towards Israel’s Talpiot training program, which is the first of its kind in the world. In March 2013, former CIA contractor Edward Snowden revealed that Pakistan was among the countries most targeted for surveillance by the U.S. National Security Agency (NSA). In June 2017, Pakistan’s Senate Committee on Foreign Affairs also warned the government that Pakistan was a principal target of cyber espionage. With Pakistan being one of the top targets of foreign espionage, there are increased calls within the country to devote more resources for securing computer systems, investing in the security of the country’s digital infrastructure, and strengthening cyber security research and development. Pakistan also needs a strong cyber security framework to counter identity theft, financial data theft, and surveillance of critical infrastructure.

While concluding his talk he said that Pakistan needs to realize the dire threat to its critical infrastructure and the government should make all out efforts to ensure the security of interconnected infrastructures of the country. For this, it is important to identify the national infrastructure that remains critical to the national and economic security of Pakistan. Pakistan needs more stringent cyber security regulations that require companies and organizations to protect their computer systems and information from cyber-attacks. The regulations should mandate government departments, the energy industry, as well as healthcare and financial institutions to protect their computer systems and information from being breached.

Dr. Nasir Mehmood deliberated upon “Cyber security in the Global Arena: An Assessment”. He started his presentation by first explaining ‘what does cyber means”. He was of the view that the word ‘cyber’ is nebulous; it means different things to different people, organizations and states. Therefore cyberspace is tricky to be perceived and demarcated. It is important to note that it is not a natural space, it is a manmade artificial space and by all means it is spooky and invisible in its nature. Cyberspace consists of a whole range of information and telecommunication related infrastructure and applications. It is fundamentally used for electronic information and communication. The real usage of cyber lies in the traditional

physical national domain which are land, sea and space and cyberspace essentially becomes meaningless without the support of these national domains. It is also profound to see that cyber is changing the context in which we used to stand and operate in the national domains of land, sea, air and space. Without a doubt cyber has integrated the time and spaces and by implication, cyberspace has challenged the conventional conception of sovereignty and borders in the realm of international relations. The ongoing pandemic has accelerated dependence and value of the information and communication across domains and sectors. In April, 2020 Microsoft Chief Executive officer Satya Nadella said that “We have seen two years’ worth of digital transformation in two months” and highlighted how every sector had to adopt and operate in a world of everything remote. More than 51% of the global population which is equivalent to 4 billion is linked with the internet and this trend is taking place with each passing day.

Talking about cyber as the exclusive domain he said that although there is rapid progress in the domain of cyberspace, there is yet an uneven distribution of cyber capabilities and resources across the regions and communities. With a solid basis of industries and technologies, the developed countries in the real world are leading and dominating the cyber domain. They are enjoying commanding positions in submarine cable network systems, internet penetrations, manufacturing of hardware and software and user servers. This cyber dominating position is helping the developed countries strengthen their positions in the real world. With a weak basis of industries and technologies, developing countries in the real world are even marginalized in the cyber domain. Such marginalization is further weakening the status of these countries in international politics. Developing countries act as mere users and developed countries act as providers of key infrastructures and applications. It is more like emergence of a classical center periphery system and accordingly states obtain their positions in the cyber domain. The purpose of security sensitizes what are the weaknesses in the defence mechanisms and consequences for the protection of the values which are at stake. Cyberspace is not perfect and vulnerable to attacks as it is essentially man made space. Cyberspace is in so many ways a double edge sword, it creates both security and insecurities cyber traditional space which are land, sea, air and space. Cyber security guards against the unauthorized access to electronic data from multiple purposes. Specifically cyber security protects the electronic information and communication against the three major sources of threats. One from viruses which happen to be in software form, second from Trojans which happen to be maliciously modified hardware and third from physical intervention of human intelligence. We may have secure computers inside secure buildings but it takes only one human to compromise the whole system.

While talking about theoretical and methodological choices he stated that the realist paradigm aspires to establish that states remain locked with the conventional agenda of national interest. However the constructivist's paradigm informs us how states are securitizing cyberspace. As for methodological choices, mixed methods are prioritized. Qualitative approaches help to understand and contextualize the intent whereas quantitative helps to quantify capabilities and generalizations across the regions.

While shedding light upon the global cyber power outlook he was of the view that as mentioned earlier cyber is spooky and nebulous, so this causes misunderstanding how exactly we have to measure global cyber power. There are few indexes available to capture the global cyber power outlook however the National Cyber power Index 2020 developed by Harvard Kennedy School is comprehensive, robust and latest one. It measures the full spectrum of intentions and capabilities that contribute to the states cyber power. By using this index states can be arranged into four groups, group 'A' includes states with higher intent and higher capabilities which include US, UK, China, France and Germany. Group 'B' includes states with higher intent but lower capabilities; among others it includes Russia, Iran, Israel and Netherland. Group 'C' includes states with lower intent but higher capabilities; among others it includes South Korea and Singapore. Group 'D' includes states with lower intent as well as lower capabilities; it includes Egypt, Saudi Arabia, Lithuania, Brazil and India. Overall the top ten cyber powers are US, China, UK, Russia, Netherlands, France, Germany, Canada, Japan and Australia.

While talking about the global cyber security outlook he said that the Global Cyber Security Index measures the commitment of countries to cyber security at the global level and its wide application across domains and fields. This index assesses 193 countries along with 5 pillars. One is the legal measures, seconds the technical measures, third is the organizational measures, fourth is capacity building and fifth is international cooperation. On the basis of the aggregate of these five measures countries are arranged into three categories, category one includes countries with higher commitment to cyber security, category two includes countries with medium commitment and third includes countries with lowest commitment to cyber security.

He concluded his presentation by stating that cyber security must be seen as a shared challenge and a shared responsibility. Collective resilience is the key to tackle the issue and the time to act is now because the adversarial use of the new technologies are coming to hunt and undermine cyberspace. Although states have been discussing cyber security issues since 1998 there is a need to institutionalize interstate dialogue on cyber security and to develop a common agenda. There is a need to develop a common language about the cyber domain. The government groups and open ended organizations must be reinforced and must be strengthened and also develop a cyber-security tool kit.

The second speaker **AVM (R) Faaiz Amir** presented his views on “India’s Quest to Dominate the South Asian Cyberspace.” He started by saying to build an understanding of the concept of dominance in cyberspace it is necessary to first understand what constitutes “cyber space”. Simply put, cyber space is a domain created by the connections between computing devices and the internet is the new category of infrastructure attracting the largest investments and attention. He asserted that the fact is cyber space is man-made but connected to the physical world drives the geography of cyber space. For example, on a minor scale our wristwatch, mobile phones, and laptops are connected to each other continuously changing the geography of the cyberspace in which we live and work, needless to say, that these devices in doing so are continuing to generate a tremendous amount of data. Another characteristic of this domain is that cyber space is fragmented into countless local areas. In a single data center, numerous systems at a different level of classification make separate local areas in cyber space. Multiple local areas can exist in the same physical location in one rag through different systems. Cyber space holds no frontier; ever-expanding cyberspace is so vast that even the largest forces are minuscule in the vastness of cyberspace. Today technologies like IoT and edge computing are enabling unprecedented levels of data generation. Cyber space is becoming increasingly an arena of nation-state conflict, much like the other four domains. The nature of warfare in cyber space has not changed but the weapons have. There is a little caveat that in the cyber domain there is little distinction between the arsenal of military and civil warriors. In cyber space, dominance is when one side can achieve its objective while preventing the enemy from achieving its objectives. However, quite unlike the other domains in the cyber space, tools and weapons are normally very specific and prevent the adversary from switching forces between defensive and offensive missions. It is difficult to move weapons in cyberspace from one area to another because cyber space weapons are specialized and designed to attack a single system. The funny aspect in this is unlike tanks, ships, and aircrafts, hostile cyber space forces do not attack each other if they cross paths in cyberspace, which makes cyberspace forces different from other forces that can detect and react to the unexpected presence of enemy forces and engage with them. Unlike land, air and maritime domains the defensive forces in cyber space do not offensive weapons once detected these are rendered impotent by patching their own vulnerabilities and updating their own detection systems. In land warfare, the defense has a legacy as a defender can stay in protection while the attacker must come in the open. In cyber space, it is the defenders that are out in the open and it is the attacker that has the advantage of cover. So the advantage in cyber space remains with the attacker who is proactive, hidden, and anonymous, while the defender is out in the open and reactive. However, that advantage of an attacker is very short-lived. Once the defender understands that he is under attack, he reacts quickly and starts the process needed to blunt the attack. At a higher level for dominating the cyber space controlling the choke points is one way of establishing universal cyber space superiority. However, it is normally not possible. A physical strike on cyber assets is considered the easiest path to lasting effects, but only if the cyber space targets are expensive and hard to replace, simple servers and computers are not productive targets. Even if bombing

attacks on infrastructure and cyber space personnel are widely effective but they do not guarantee the overall victory in the conflict.

As earlier mentioned in cyber space the geographic separation of theaters of war is not a significant factor as players may have a server and nodes spread over the entire globe. Thus, to achieve cyber space dominance an attacker might have to achieve a dominance all over the cyber space, which is not realistic instead a combatant achieve a significant military advantage for military operations to local cyber space superiority. So, for cyber space superiority, local area superiority is more fundamental than total space domination. In the cyber space domain, both attackers and defenders will do the vast majority of their battles at the system level. An attacker will gain control of the local area by sneaking into the system. However, this local superiority may not be persistent because of the backups. Hence, they are replicable; this replicability makes dominance or superiority very short-lived and allows rapid recovery from the attack. The one case in which attackers managed a significant persistence measured in years was Stuxnet Attack on Iranian nuclear facilities because the weapon remained hidden for very long and defenders did not know they were under attack. Dominance in cyberspace is useless if combatants cannot translate this dominance into complete gain. So, the combatants have to successfully achieve the linkage of mean, goals, and ends. Analysts believe that in a conflict most important offensive contribution of cyberspace would be an enabler of forces in other domains. AI has demonstrated a collaborative relationship in the battlefield, where an AI agent handles tactical tasks while the onboard human focuses on the higher-level strategy as a battlefield manager who is supervising multiple platforms. As forces become increasingly reliant on cyberspace tools and connectivity such as target tracking systems, remotely piloted vehicles, and data links. The accomplishment of cyber space brings significant advantages for combatants at tactical, operational, and strategic levels of war. AVM (R) Faziz Amir quoted Martin Libicki with “cyber space biggest contributions will be in support of forces in other domains instead of in strategic domains of strategic information warfare” He said that historically technology has played a significant role in shaping the character of war. Cyber space is a high technology domain and there is always and the temptation of chances of technological determinism that is success in cyber space would be determined by technological innovations. He further argued that it is unrealistic to believe that any attack in the cyber space domain would completely hamper the ability of nation-state to resist.

Lastly, he explained the Indian ambition to dominate the cyber space. He said that the Indian technological and IT industry is to grow by 7.7 % this year and it earns the revenue of USD 1.91 billion. Currently, it accounts for over 8% of the share in India's GDP and has a significant role in offsetting Indian import bills. The industry has a workforce of 4.36 million people, with adding 2 million employees/people in only the last decade. Indian military benefits from this large pool of talent. The industry today boasts companies with annual revenue of USD 1 billion and 24 startups have attained a unicorn status. Indian expects over 50 startups, and these startups are growing by over 15 % in the last five years. With ICT exports of 85 billion USD, Indian is already ranked 1 in 124 countries, ahead of China which ranks at 5th position. These figures indicate India's quest to dominate regional cyberspace. With the new cyber security policy of India that is expected this year, it aims to build resilient and secure cyberspace for citizens, businesses, and governments. These developments would provide India with a large man and technical force and there is a lot to learn from it. To summarize the cyber space is a huge and unique domain where normal principles of war do not apply. However, unlike other domains, a total dominance of cyber space is yet not attainable and not even required to achieve objectives whether in strategic information warfare or support of other domains. States will attack each other in local area networks and will cause disruptions there for their adversaries. In this segment, India has a large pool of competent technical force to be a factor in any future armed conflicts.

The last speaker, **Dr. Tughral Yamin** deliberated upon "State of Cyber Security in Pakistan: Emerging Threats" where he emphasized that Although security ranks high on Pakistan's national agenda but in the increasingly complex threat milieu, cyber security usually gets relegated to the bottom rung and sometimes it is literally ignored. There is no gainsaying

the fact that we ignore this vital subject only at our own peril. Given the chaotic nature of cyberspace, it is important to manage it properly. The Internet has its advantage. It has made the availability of knowledge at the click of the button. Connectivity has made life simpler on different planes, ranging from the personal to an official, but has also introduced several vulnerabilities. Access to the Internet is now considered a basic human right. At the same time, cyberspace has become the fifth dimension of warfare. In the absence of international cyber treaties and agreements, states are actively carrying out pervasive surveillance against friends and foes and launching devastating cyber-attacks. Terrorists are using cyberspace for recruitment, funding, and propaganda. Criminals are having a field day in siphoning off millions of dollars from online e-commerce activity; the kids in the basement and freelancers high on digital adrenaline are hacking just for the kicks of it.

Such threats need to be responded to by coordinating cyber security activities at the national level. Robust cyber governance bodies need to be created at all levels. Cyber leaders and advisors need to craft effective policies and enact legislation to counter the ill-effects of debilitating cyber-attacks i.e., disruption of communication services and damage to command and control systems that cause the government to malfunction and make the businesses and industry lose hours of productivity among other things. Unfortunately, Pakistan is way behind other nations in putting its cyber act together.

Data security in Pakistan is unfortunately not at the top of either the national or any organization's agenda. There are regular reports of databases being breached. Officially Pakistan does not have a national policy on cyber security. Pakistan is one of the most cyber spied upon countries in the world. It is not India alone that wages a strong cyber offensive against Pakistan, many other countries are using cyber means to syphon off critical data. The US is one of those countries that actively and regularly spies upon Pakistan.

There are clearly identifiable hurdles in establishing a meaningful cyber security architecture in Pakistan e.g. there is no central authority to coordinate on cyber security matters and advise the prime minister about emerging cyber threats. There is a palpable lack of awareness within the policymaking circles. Apart from the cybercrime bill, there is no clear cut policy on the subject of cyber security. The cyber security stakeholders are not clearly defined and their turf is not properly marked out. There is no PK- CERT and no funds allocated for cyber security purposes. The Federal Investigation Agency (FIA) has a National Cyber Response Centre for Cyber Crime (NR3C) but its mandate is limited and it lacks the wherewithal to act as the first responder in case of a computer. Pakistan is represented at the UN Group of Governmental Experts on Information Security (Crime), but the national point of view expressed on these forums is not shared with the public.

Pakistan has a very huge and talented human resource. The only thing that we lack is direction and policy and that is not possible without good cyber managers and planners. Most people at the top echelons of the security establishment lack the knowledge and vision to properly organize cyber security. Crash courses in cyber awareness to senior government officials and parliamentarians can go a long way in improving the cyber security milieu in Pakistan. Courses can be taught in cyber security management in the universities and they can be made part of the curriculum of the much-vaunted National Defence University (NDU) security workshop. First and foremost, there is an urgent need for well-defined national cyber security architecture. The powers of coordinating all issues related to cyber security may be vested in the office of a cyber-security coordinator working directly under the prime minister. He may be provided secretarial services by the NSC. The NSC could be one forum, where all cyber security measures may be discussed. Second, a cyber-task force (CTF) as suggested by Senator Syed may be placed under the NSC. The mandate of the CTF should include issuing policy guidelines on cyber security. Third, the creation of PK-CERT is a long outstanding issue. The national CERT should be established and asked to practice cyber emergencies on a regular basis. Fourth, cyber funds should be allocated in the national budget, and their proper utilization ensured by the national cyber security coordinator. Fifth, cyber security cooperation with other countries, particularly those belonging to the South Asian Association for Regional Cooperation (SAARC) would have been ideal but unfortunately, this association has become moribund due to Indian intransigence. Pakistani FO may consider raising the issue of regional cooperation in cyber security at the forum of Shanghai Cooperation Organization (SCO). This cooperation should be meaningful and expand beyond the brief reference made in the joint statement issued after the visit of the former Prime Minister Nawaz Sharif's visit to the White House in 2015.61 Last but not least, a cyber-security debate in the parliament may help set up a long term plan. It would be a good idea for political parties to have cyber security issues included in their election manifestos.

Observations and question & answers session:

Air Commodore (R) Khalid Banuri, (Former DG ACDA) while giving his comments on Dr. Nasir Mehmood's talk maintained that Cyber Domain may be nebulous, but several aspects are pretty much tangible. He further added that shared challenge and shared responsibilities are noble intent, but this would not happen due to realpolitik. He also asked a question to AVM (R) Faaiz Amir How much of successful defence or attack is dependent on time-space relationship? What kinds of timelines are involved, days, hours, minutes, and seconds? While responding to his question, AVM Faaiz Amir (R) said that the time-space relationship is actually irrelevant in the domain of cyber security. Since the successful attack in cyber security can be malware when it hits the system in which it is already sitting there for months or years and it activates itself on a given time. Thereafter, the reaction of the defending site is dependent on its preparedness to answer such attacks. So the attack on the system cannot take place unless the malware is already hiding there for quite some time. For reference, if we buy hardware and malware is already sitting inside like for instance the cellular phones and other systems that we get from other countries. The US' ban on Huawei's has enhanced the tensions between the US and China. Since the latter is suspected by the former of sending malware and spying on the US' communication systems through 5G devices. This implies that the timeline is breached already and the time-space relationship has not much relevance vis-à-vis cyber security.

He also gave his comments on Dr. Tughral Yamin's presentation, by saying that most of the vulnerabilities that you have covered perhaps existed for a very long time even when cyber security was not the buzz word. Some of them have now become more important and that is quite understandable. He raised a question to him as well: How to deal with the challenge of

Big Data Management? Dr. Yamin very simplistically responded by saying not to store all your data in one place.

Mr. Zafar Iqbal Yousazai, (Senior Research Associate, SVI) asked a question to Dr. Nasir Mehmood that when it comes to traditional warfare between India and Pakistan, nuclear weapons work as a source of deterrence, However in the case of cyber security what can be the source of deterrence between both states? Dr. Nasir responded by saying that it is very tricky to determine cyber deterrence in third world countries. Since the main purpose of deterrence is to prevent a war, in cyber security it would be very difficult to determine the ideal cyber deterrence between any two states.

Ms. Adeela Ahmed (Research Fellow, PICS) asked a question to Dr. Tughral Yamin. The significance of cyber security has somehow remained less significant, what can be the policy options to be considered by the government in this regard? While responding to her question, Dr. Tughral termed it very relevant and said that at forums like the SVI we need to talk more about cyber security. He further suggested, for the next time, the SVI may kindly invite people from the government for instance the Minister of Information Technology or some other government officials who can sit and listen; this seems to be the only way that is needed to be deliberated.

Ms. Sadia Kazmi (Director Academics, SVI) asked a question to AVM (R) Faaiz Amir. As Pakistan is one of the most targeted countries in the world in the cyber domain wherein most of the attacks are coming from India, do you think this offensive cyber posturing could raise the escalation risk in South Asia? Are there any prospects of cyber diplomacy between India and Pakistan? Have the two countries been engaging or thinking on these lines? While responding to the question AVM Faaiz (R) Amir said that definitely cyber-attacks can increase the escalation risks in South Asia as I have said the cyber domain is yet another domain and there are cyber weapons that can cause grave harm to the national assets and the decision making process. It has the potential to escalate into other domains as well. Regarding cyber diplomacy, he maintained that there is a possibility since both countries have successfully established nuclear diplomacy. There appears to be no reason that both countries cannot reach a minimum understanding of cyber ethics. However, the nebulous nature of cyber space cannot be ignored in the case of India and Pakistan since an Indian cyber-attack on Pakistan can originate from any country where the Indian’s have a presence.

Mr. Husssain Muhammad (HEC Fellow in IR, QAU) raised a question for AVM (R) Faaiz Amir. Is it plausible to see that we need overarching cyber security training starting from early childhood education particularly the social engineering side of cyber security? While responding, AVM (R) Faaiz Amir said that social engineering is the one great vulnerability that cyber systems carry. It is happening in many countries including Pakistan that hackers are involved in data breaches through social engineering. There is a requirement of educating the general masses who use telephones and work on computer systems. For children, he recommended keeping them away from screens till a certain age.

Ms. Ahyousha Khan (Senior Research Associate, SVI) asked a question to Dr. Tughral Yamin. What is the main reason behind the inability of Pakistan to formulate a comprehensive cyber security policy or strategy? Dr. Yamin said that there are various hurdles like for instance governments are always occupied in many other things, sometimes the government is not willing to give much-required attention to this domain. AVM (R) Faaiz Amir added one reason is that we do not have a very large formal IT sector. The IT companies are not powerful enough to demand from the government a cyber-security policy. The government needs to take measures which would allow the private sector to grow and start being a factor in this domain. Furthermore, there are competing forces within the government and states that have delayed the formulation and finalization of cyber security policy.

Mr. Haris Bilal Malik (Research Associate, SVI) raised a question for AVM (R) Faaiz Amir, How do you see the future of Cyber Space security in South Asia? He responded by saying that it is something that is not going away. The IT industry is growing faster and Pakistan is witnessing kind of an upsurge in IT technologies. As the usage at the public level expands there would be more cyber experts in the country. The only thing that would make difference is the cyber defence against the outsider's threats.

The last question was raised by Dr. Zafar Iqbal Cheema (President/Executive Director, SVI) and it was directed towards AVM Faaiz Amir. He referred to the official website of Pakistan's Ministry of Foreign Affairs which was hacked in February 2019. Furthermore, the website of the public relations wing of the Pakistan Navy in October 2019 was also seized reportedly from the Indian sources. How much significant they were? AVM Faaiz Amir responded by saying that he is not aware of the inside news, but sometimes these attacks are to check on your defensive systems to identify vulnerable targets. These attacks occur in a manner to check the capability of the system that in case of the actual attack the hackers would probably know the lope holes in the system.

In the end, Dr. Zafar Iqbal Cheema (President/Executive Director, SVI) thanked all the panelists for their comprehensive presentations and for making their distinguished contributions. He also thanked the participants, who have joined the webinar and raised very significant questions.

Media Coverage:

The Coverage of the SVI webinar was reported in print, electronic, and streamed live on social media. The recording is also available on the SVI official YouTube Channel.

PTV World News

https://www.facebook.com/585117914834456/posts/4017880234891523

DAWN

https://www.dawn.com/news/1604574

YouTube

https://youtu.be/L7ve8lFsbHg