INSTITUTE OF STRATEGIC STUDIES

web: www.issi.org.pk
phone: +92-51-9204423, 24
fax: +92-51-9204658

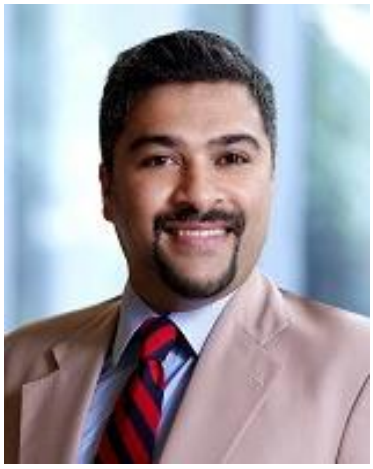
Report – Webtalk

"Changing Global Dynamics of Cyber Threats and their Impact on National Security"

September 11, 2020

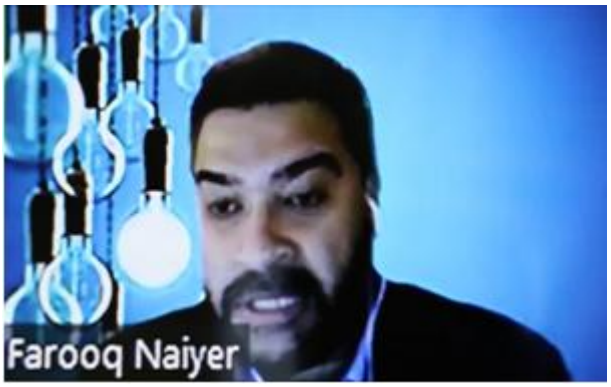
By

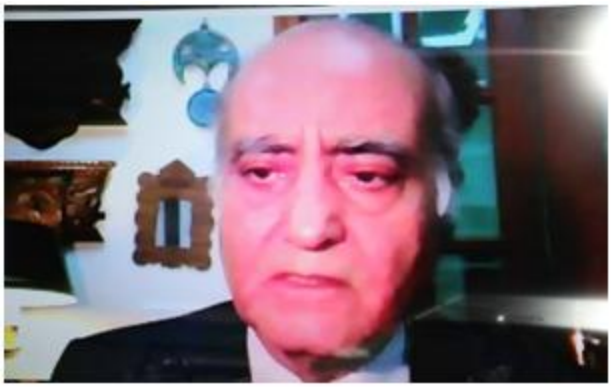
Mr Farooq Naiyer,
Cyber Security Expert from Canada

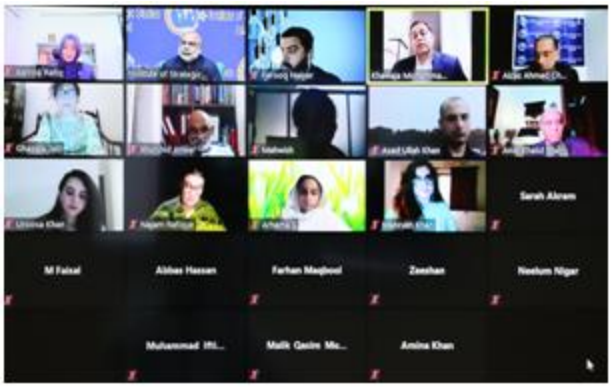


Compiled by: Ghazala Jalil *Edited by: Malik Qasim Mustafa*

PICTURES OF THE EVENT







The Arms Control and Disarmament Centre (ACDC) at the Institute of Strategic Studies, Islamabad (ISSI) organised a webtalk on "Changing Global Dynamics of Cyber Threats and their Impact on National Security," held on September 11, 2020. The webtalk was delivered by Mr Farooq Naiyer, a cybersecurity expert from Canada. Mr Malik Qasim Mustafa, Director Arms Control and Disarmament Centre (ACDC), moderated the event. Ambassador Aizaz Ahmad Chaudhry, Director General ISSI, opened the event with his welcome remarks. Mr Khawaja Mohammad Ali, Chief Information & Cyber Security Officer, Agriculture Development Bank of Pakistan (ADBP), Islamabad, was the first discussant and Ms Aamna Rafiq, Research Associate ACDC, was the second discussant. The closing remarks were delivered by Ambassador Khalid Mahmood, Chairman Board of Governors, ISSI.

Introductory Remarks by Malik Qasim Mustafa, Director ACDC-ISSI

In his introductory remarks, Malik Qasim Mustafa said that since the last decade the cyber threats have started to emerge as a significant risk to national security and with time, the technological advancements in cyberspace and its growing integration with the political, social, cultural, economic and military domains, has made states vulnerable against cyber threats. Especially, after the COVID-19 pandemic states are greatly exposed to existing and emerging waves of cyber threats.

With time, he said, that the dynamics of cyber threats have also changed. The nature of such threats has transformed from a common cyberattack or hacking incident by an individual or group to the development of defensive and offensive cyberwarfare capabilities by states. And there is a race to become the world's top cyber power e.g., the US, China, Russia, Israel and the United Kingdom are the leading cyber powers. There are reports of powerful states cooperating with other states to carry out large-scale attacks against other states. For example, the Indian cyberattack threats are growing against Pakistan. There are reports that India with the cooperation of Israel has stepped up its efforts to strengthen its offensive cyberwarfare capabilities against Pakistan. According to December 2019, *Guardian* report "Israeli spyware allegedly used to target Pakistani officials' phones." Most recently in August 2020, the ISPR said that the Pakistani intelligence agencies had identified a major cyber-attack by the Indian intelligence agencies, targeting the mobile phones and gadgets of government officials and

military personnel. Such developments highlight that these shifting dynamics of cyber threats would seriously affect national security.

With this premise, the ACDC at the ISSI has organised this webtalk on "Changing Global Dynamics of Cyber Threats and their Impact on National Security" to explore the answer of following questions.

I. What are the changing global dynamics of cyberspace and what kind of cyber threats are emerging?

II. How these cyber threats are going to impact international, regional and national security?

III. And how we can mitigate these threats and help formulate policy-relevant recommendations for greater cooperation and engagement?

Welcome Remarks by Amb. Aizaz Ahmad Chaudhry, Director General ISSI

Ambassador Aizaz Ahmad Chaudhry said that in the contemporary security landscape, cyberspace is a strategic asset which is being used by a variety of interconnected actors for a variety of purposes like e-governance, e-banking, e-commerce, communication, etc. This increasing dependency is not only creating new avenues of cooperation and opportunities but also making us more vulnerable to a variety of new threats. The threat spectrum in cyberspace ranges from low-level individual crime to serious crime by political and ideological extremists' organisations with or without state sponsorship.

He said that since the start of coronavirus pandemic, we have seen a massive wave of cyber-attacks. The World Health Organisation (WHO) has reported a five-fold increase in cyber-attacks. Earlier in this week the spokesman of the Atomic Energy Organisation of Iran (AEOI), Behrouz Kamalvandi, announced that Iran had stopped a large number of cyber-attacks targeting its nuclear facilities. Last month, the Inter-Services Public Relations (ISPR), reported a major cyber-attack by the Indian intelligence agencies. The Indians were involved in hacking personal mobiles and technical gadgets of government officials and military personnel. Several banks in Pakistan were hacked causing huge economic losses.

The situation of global as well as national cyberspace is extremely critical and it must be handled. The response should be appropriate, effective, efficient and above all as swift as possible. But the first step is moving from reactive mode to pre-emption.

He emphasised two key questions to be pondered upon:

I. What are the emerging threats in cyberspace that will lead to shifts in national security?

II. What policy choices and infrastructural options do we have?

Webtalk by Mr Farooq Naiyer, a Cyber Security expert from Canada

Mr Farooq Naiyer said that both state actors and non-state actors are operating in cyberspace and using offensive cyber capabilities which have blurred the line between threats posed by states and non-state actors. In the majority of cases, civilian infrastructure is targeted. He broadly spoke of four elements regarding cybersecurity - current threat landscape and trends; what is in the headlines; how is Pakistan positioned? and recommendations.

Talking about the current threat landscape he said that wholesale trade has been hit, as well as the chemical manufacturing sector. He emphasised that telecommunication is the field mainly under attack from cyber threats. These include wired telecommunication carriers, telecommunication, data processing and related services and wireless communication. He identified three kinds of threats - banking trojan, malware downloaders and ransomware. In the cyber world, there are mercenaries that governments and entities can hire.

In recent years and months, there have been cyber-attacks on major infrastructure in New Zealand, Australia, Israel, Iran, as well as Pakistan. He pointed out that cyber threats have gone up many-folds across the world and can affect Pakistan as well. In this regard, Pakistan is taking actions to deal with cybercrime and cyberthreats but needs to take more organised action. In recent years there has been an increase in ransomware attacks. This is an organised criminal gang that has been targeting governments. These work like mercenaries that are available for hire to conduct attacks. At times nation-state hires mercenaries to conducts cyberattack on their behalf. The private sector is also vulnerable to them.

He also highlighted that cyberthreats are linked with the evolving geopolitical situation. Tensions between India and Pakistan, foreign policy choices and the evolving Middle East situation are all linked with cyberattacks. Calling it the 5th generation warfare, he said that potential targets in Pakistan could be critical government and private sector infrastructure, as well as strategic initiatives like China Pakistan Economic Cooperation (CPEC). He stressed that cyber threats are a clear and present danger and we need to organise ourselves to deal with it.

He noted that the National Cybersecurity Policy and Framework are working on the issue of cybersecurity but much more needs to be done to deal with this threat. He emphasised that leadership in the public and private sector must posture their organisations for a growing risk of surprise in cyberspace by setting up Cybersecurity Incident Response Teams (CSIRTS) across various departments and organisations. The government and private sector must train cyber incident response professionals in the area of cyber threat intelligence. He also pointed out that threat intelligence will need to evolve from incorporating indicators of compromise gleaned from detected cyber activity. He also stressed the need to take proactive measures to increase the operational and technical resilience of organisations. Government entities, researchers and think tanks can likely assist public and private sector organisations in posturing for this new environment by developing standards and template processes for using the geopolitical analysis to drive cyber defence. Senior executives can prepare their workforces for this environment by developing a consistent and multi-dimensional communications strategy used at all management levels He said that new approaches for government and private sector collaboration must be created to ensure national security as private sector firms increasingly become “front line” targets for foreign actors. Repeatable collaboration processes should define the roles and responsibilities of private firms and the various government entities that have a role in protecting national security and conducting law enforcement.

Discussant I: Khawaja Mohammad Ali, CICSO ADBP, Islamabad

Khawaja Mohammad Ali said that warfare has moved from air and land to cyberspace. There is a serious need for civil-military cooperation to tackle this issue. There is a need to pursue a regional approach toward cybersecurity. In conventional warfare, a military triad can operate independently and safeguard our physical borders. But cyberspace has no boundaries. Most

activities of a nation are now conducted in cyberspace. Thus, there is added responsibility for the military to safeguard cyberspace as well. Hence civil-military cooperation is imperative. That has to be done with the right strategy.

Talking about the importance of the region, he said that with the CPEC coming in and other trade and economic activities, it also brings more vulnerability in cyberspace. The whole scenario is being changed regionally and globally. We, thus, have to ensure our defence capabilities in the cyberspace. State and non-state actors are both a threat that poses dangers to the banking and energy sector. It can affect businesses like Uber and Careem and the entire cyber ecosystem. We, thus, need to develop cyber defence by protecting our critical infrastructures.

In this regard, he recommended aligning with friendly countries to tackle the issue of cybersecurity and tap into their expertise in this area. He also highlighted the need to exercise cyber diplomacy and dialogue. He said Pakistan needs to align with the rest of the world in cyberspace. This is one realm where there are no geographical boundaries. Cyberattacks were not a matter of if they will happen but rather when they will happen. Thus, Pakistan needed to be prepared for it.

Discussant II: Ms Aamna Rafiq, Research Associate ACDC-ISSI

Talking about the current debate vis-à-vis establishment of an international regulatory regime in cyberspace, she highlighted the complex issues of proliferation and misuse of cyber technologies by state and non-state actors. Over the years, there have been efforts to regulate cyberspace and the establishment of a cyberspace regime has been on the UN agenda since 1993. However, states could not achieve consensus on fundamental issue areas. There are three main intricate challenges which are hindering the development of an international consensus. The first challenge is the difference of cyber ideologies among states. States which consider cyberspace a global common are in favour of open and free access to cyberspace. However, states in favour of cyber sovereignty want to regulate cyberspace according to their national laws. The second challenge is the applicability of existing international laws. Some argue that existing laws are applicable to all issues ranging from cybercrime to an armed conflict while others argue that a new set of laws are needed for cyberspace. While favouring the latter approach, she said that the existing legal regime is adequate to deal with the complex issues of attribution and armed

conflict in cyberspace. She also expressed her concerns regarding the misuse of international humanitarian laws by powerful states to impose digital sanctions on weaker states. The last point she made is that states have to determine the threat threshold while keeping in view the sensitivity surrounding the relevance of Article 51 of the UN Charter in cyberspace. India is trying to introduce a new normal of a limited war under the nuclear threshold. India has also introduced a new triad of cyberspace, outer space and surgical strikes in its Indian Armed Forces Joint Doctrine, 2017. In this regard, India can use the pretext of a cyberattack to launch a surgical strike on Pakistan.

While supporting the idea of a regime complex in cyberspace, she suggested that instead of forming a large cyberspace regime, smaller regimes that deal with an individual domain like economic, financial, military and critical infrastructure should be established. The basic objective is to design a comprehensive regime comprised of a small and specialized regime with a specific level of coherence and overlap.

Question and Answer Session

Q: Where does Pakistan stand in terms of cybersecurity?

A: Pakistan lacks a coherent cybersecurity strategy. The government is working on establishing a formal, coherent cyberspace policy. The private sector has its cybersecurity setup. However, efforts between the government and the private sector are not coordinated. Civil-military cooperation in this domain is also needed.

Q: What are the readiness challenges?

A: There is a need to have a unified cybersecurity policy and framework. Also, practical steps are needed to implement the policies. Cyber intelligence sharing between organisations and the private and government sector is vital as far as cyberthreat readiness is concerned.

Q: What will a cyber incident response will mean for medium-sized organisations in terms of resources and technology?

A: For medium-sized organisations, cyber incident response is not a cost-intensive thing. It would include things like effective antivirus and a good windows system for computers.

Technology is already owned by us; it is a matter of organising it and implementing it effectively. On a broader level, Pakistan should adopt a regional approach allying and partnering with friendly countries and tap into their expertise.

Concluding Remarks by Ambassador Khalid Mahmood, Chairman BoG ISSI

In his concluding remarks, Ambassador Khalid Mahmood said that the technology is inexorably progressing. He quoted the Russian President, Vladimir Putin, who said that a nation that leads in artificial intelligence will lead the world. The effect of new technologies is being felt all across the world. Also, the concept of security has expanded. Cybersecurity is now part of national security that is all-encompassing. He said that there are so many actors that are involved in cyberspace including governments, civil organisation, non-state actors and terrorists.

Threats in cyberspace are having an impact on conventional military defence and perhaps on nuclear capabilities. He said that India and Pakistan as nuclear weapon states are vulnerable to cyberattacks. Unless the threat is managed, it has the potential to undermine strategic stability. He emphasised the need to have rules at national, regional and international level – the world must agree on common rules of engagement. These rules have to involve government and civil sectors. He said that he is hopeful that there will emerge a coherent response to cyberthreats. In the past, as well there have been disrupting technologies but the collective wisdom of the international community rose to the challenge to regulate it. He reiterated, thus, the need to have laws at the national, regional and international level to manage cyber threats.