INSTITUTE OF
STRATEGIC STUDIES

web: www.issi.org.pk
phone: +92-920-4423, 24
fax: +92-920-4658

Report – Panel Discussion

"Cyber Technologies and Responsible State Behaviour: Achieving Peace, Security and Sustainable Development"

June 29, 2021

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

The Arms Control and Disarmament Centre (ACDC) at the Institute of Strategic Studies, Islamabad organised a webinar on "Cyber Technologies and Responsible State Behaviour: Achieving Peace, Security and Sustainable Development" on June 29, 2021. The eminent speakers included Brig. Mohammad Yasin, Senior Advisor SDPI, Dr Tughral Yamin, Associate Dean CIPS, NUST and Dr Khashif Kifayat, Dean Computer Sciences, Air University Islamabad.

Introductory Remarks by Malik Qasim Mustafa, Director ACDC-ISSI

Malik Qasim Mustafa said that the use of cyber technologies or commonly known as computers, cell phones and other devices which are connected with the internet have been working as "agents of change," for decades. These technologies have transformed our lives and providing us with endless possibilities to transform our future. The ongoing pandemic has made us realised that how these cyber technologies are playing an important role in connecting us and how they can bring social, economic and political change to our lives. According to a recent World Economic Forum report, there are around 300 technologies that can directly support 70 per cent of the 17 sustainable development goals and almost 80 per cent of these technologies are internet dependent. However, it is important to note that access to such technologies and their use sometimes creates complex challenges.

He noted that as the frequency and lethality of malicious cyber activities have increased manifold, cyber technologies are going to change state behaviour in major ways. The world is already witnessing a growing competition between major players to dominate each other in cyberspace. There is a likelihood that this growing use of cyber technologies would affect individuals and states and peace, security and development. In this regard, states should ensure the protection of cyberspace from cyber threats and cyberwarfare to safeguard their social, economic and national security interests. For that purpose, it is important to raise awareness, design cybersecurity culture, develop cyberspace norms and design legal regimes at the national, regional and global levels for regulating cyber technologies to achieve peace, security and development.

He also highlighted the objectives of the webinar:

1. Identify the issues related to malicious activities in cyberspace and their implications on peace, security and sustainable development.

2. Analyse the various ways to enhance responsible state behaviour in cyberspace.

3. Bring together the national strategic community for policy discourse and help formulate policy-relevant recommendations for security, peace and sustainable development in the new cyber age.

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

Ambassador Aizaz Ahmad Chaudhry in his welcome remarks said that cyber technologies are changing the way humans lead their life. Its use can be positive or negative. It is the malicious use that is of concern. Need to regulate it at the regional and global levels. It is important to generate debate on responsible state behaviour in the cyber realm.

Briefing by Ms Aamna Rafiq, Research Associate ACDC-ISSI

Ms Aamna Rafiq said that as part of "Frontier 2030: Fourth Industrial Revolution for Global Goals Platform," the World Economic Forum published a Report on "Unlocking Technology for Global Goals" which showed that based on current applications, Fourth Industrial Revolution technologies could have a high impact in particular across 10 of the goals. She said that 70 per cent of the 169 targets underpinning the goals could be enabled by existing Fourth Industrial Revolution technology applications. These technologies are Artificial Intelligence, Quantum, drones, the main cyber technologies included in this report are the Internet of Things, Big data, 5 G, Augmented Reality. All these technologies are exceptionally interlinked and act as a building block for each other. However, more than 80 per cent of the technology applications identified across the goals rely on internet access. Cyber technologies facilitate increased productivity of systems; enabling transparency and stakeholder accountability; aiding the shift to decentralised systems; supporting new models to unlock finance.

She highlighted that while there is an enormous opportunity, some important barriers remain. These include poor data access and quality, a lack of basic infrastructure and inadequate governance and policy environment, upskilling and reskilling needs. Then, there is a risk of proliferation of cyber technologies and misuse by the state and non-state actors. To achieve the SDGs by utilising cyber technologies, it is essential to establish an international regime to regulate cyberspace and promote responsible state behaviour. She noted that after more than 20

years of rigorous effort, debate and initiatives, the negotiations for the international legal regime for cyberspace are still in the doldrums. Previously, states successfully negotiated international legal regimes on a range of complex fields like nuclear, outer space and high seas but now they are unable to reach a consensus on cyberspace. Various intricate issue areas are hindering the development of this consensus like the Difference of Cyber Ideologies, the Applicability of Existing International Law and what should be considered as an armed conflict in cyberspace. This threshold will be different for different states. The threshold determination is extremely important especially when we talk about the applicability of Article 51 of the UN Charter on the Right of Self-defence.

In conclusion, she said that it is critical to identify new ways to unlock the full potential of cyber technologies for human development. Keeping in view the risks and challenges, we do not have the luxury of time. It is time to take quick action instead of celebrating promises. Developing technology is no silver bullet but these developments could be an essential building block in the ability to achieve the Global Goals in 2030.

Remarks by Brig. Mohammad Yasin, on "Cybersecurity for Sustainable Development"

Brig. Muhammad Yasin said that there has been a rapid increase in cyber-attacks globally over the last few years. There is a deep relation between cybersecurity and growth and development. Cybersecurity is vital in achieving sustainable development goals. However, the digital economy can only grow if the IT infrastructure is secure and resilient and enjoys the trust of people. Pakistan has many challenges in the realm of cybersecurity. Pakistan's capacity to deal with them is weak. According to the global cybersecurity index, Pakistan ranks at 94th place. The report highlights that Pakistan lacks the capacity to counter cyber attacks. He said that Pakistan's cybersecurity posture is weak, disorganised and superficial. Public and private organisations are working in isolation. There is no coordination between the armed forces of the country, no cybercommand to plan and implement cyber SOPs. This is essential, he said, because hybrid wars are now replacing conventional wars. He emphasised the need to work to secure the country's infrastructure. Vulnerability threats must be identified and solutions devised. Pakistan now has a cybersecurity policy put out by the Ministry of Information Technology and Telecom. It aims to set up a national body to regulate all cybersecurity matters. All stakeholders must work together to devise best practices. He stressed that there can be no sustainable development

without cybersecurity. Cybersecurity will impact three pillars of development – the economy, governance and human security which are enshrined in the sustainable development goals.

For policy recommendations, he said that emerging technologies must be harnessed for sustainable development. He said that strong cybersecurity task force development by training manpower is crucial to progress in the economic and social spheres. Dynamic planning exercises and simulation, vulnerability tests are a must. The establishment of a Tri-service command is essential to optimise security efforts in defence forces. National cybersecurity entity must be effectively deployed. Most important of all, international collaboration is imperative because cyber threats are a global menace. Thus, collective efforts are needed.

Remarks by Dr Tughral Yamin on "Building a Cyberspace Regime for Security and Peace"

Dr Tughral Yamin, talking about essential components of a cybersecurity regime, said we need a regional approach that is possible since we do not have a coherent national approach at present. He said the cyberspace regime should be part of the overarching national security architecture. He suggested that it should have joint ownership of all the stakeholders including the military-civil sector and corporate sector. It should cover all legal aspects but should not be at the cost of the citizens' digital rights. He said it should be adopted with consensus through the parliament.

He said that cybersecurity should be on top of the national and global agendas. He said that a regional approach is possible through SAARC or Shangai Cooperation Organisation (SCO). The SCO is a better forum because it is not hostage to India Pakistan rivalry. He suggested Cyberspace CBMs between India and Pakistan.

Remarks by Dr Khashif Kifayat

Dr Khashif Kifayat shared his views on "International Cooperation for Peaceful Uses of Cyber Technologies: A Case for Pakistan." He said that cyberspace is composed of the internet, computer systems connected and helping us do our day to day work. He said that in today's world cyberspace is increasingly important because our dependence is increasing. The economy, industry and other sectors are digitising and moving into cyberspace. He talked about the human factor in cybersecurity. He especially talked about online child exploitation that is hitting the

entire world very hard. He said that this can be a common ground for international cooperation. A lot of countries have advanced cyber technologies to catch cybercriminals. However, they are banning Pakistan from using these technologies. This gives a negative message. However, a cooperative approach is imperative to combat the menace of child exploitation online. Another area where global cooperation could be very fruitful is the banking sector. This is a sector where we can collaborate internationally to stop cyber crimes which cause financial losses. He emphasised the need to develop human resources in Pakistan to tackle the problem of cybersecurity.

The approach we have taken so far is that the National Center for Cyber Security was formed in 2019. The purpose was to develop technologies to protect Pakistan's national assets. Its main focus was R&D. At Air University we have R&D and have developed an eco-system. We need to have a proper education system, a training system and human resource development to sustain a system of cybersecurity. Another component of the ecosystem is the development of the cybersecurity industry. The purpose is not just for Pakistan to benefit but to share the benefits of cyber technologies internationally. In this regard, Air University has devised a Bs, Masters and PhD curriculum in cybersecurity which is now being followed in over 20 cybersecurity programmes all over Pakistan. Thus, developing human resources in the realm of cybersecurity is imperative.

Question and Answer Session

Q: Is there a cybercrime unit at Federal Intelligence Agency? What is the focal point in Pakistan for stopping malicious use of cyberspace?

A: The FIA has a very limited force and capacity to control cybercrimes. Overall, Pakistan's capacity to control cybercrime is extremely limited.

Q: How the phenomenon of nation-states investing in offensive cyber capabilities is impacting sustainable development? What was the trend in South Asia?

A: Cybersecurity has to have a regional cooperation mechanism and global mechanism. This needs the active involvement of the United Nations. Regionally the adverse relations between India and Pakistan and Iran and Saudi Arabia are hampering any cooperation on cybersecurity.

Unless there is a change like relations between these countries a regional cooperation mechanism cannot be negotiated.

Q: The issue of cybersecurity is being discussed in the UNSC for the first time how do you see it?

A: Endorsement from the UNSC over the issue of cybersecurity is certainly a good step. However, oftentimes an agreement is reached on an action plan but it is not implemented.

Q: What about Pakistan's cooperation with China in the cybersecurity domain?

A: There is cooperation at the level of universities and a few MoUs have been signed. Pakistan is also working with the UK, Germany to increase cooperation on cybersecurity. Pakistan needs to build trust at the international level to achieve fruitful cooperation in the realm of cybersecurity.

Concluding Remarks by Amb. Khalid Mahmood, Chairman BoG ISSI

Ambassador Khalid Mahmood said that cyber technologies can help accelerate the achievement of the UN's Sustainable Development Goals. They are also helping in peacekeeping efforts and better governance. There are great benefits to cyber technologies but it has its costs. These techs can be misused to launch like cyberattacks. These threats are increasing in sophistication and inflicting major financial losses to countries corporations and individuals. He pointed that access to cyberspace and its misuse by non-state actors is a source of concern and can create havoc. As cyber technologies keep evolving, so there is a need to promote measures to promote responsible behaviour in the form of a legal framework, awareness and skill development.

PICTURES OF THE EVENT