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

Report – Webinar

"Securing Pakistan's Cyber Domain: Challenges and Opportunities"

March 16, 2022

Rapporteur: Aamna Rafiq *Edited by: Malik Qasim Mustafa*

The Arms Control and Disarmament Centre (ACDC) at the Institute of Strategic Studies Islamabad (ISSI) organised a webinar on "Securing Pakistan's Cyber Domain: Challenges and Opportunities" on March 16, 2022. The webinar was moderated by Malik Qasim Mustafa, Director, Arms Control & Disarmament Centre (ACDC).

Welcome Remarks by Malik Qasim Mustafa, Director, ACDC

The growing reliance on cyberspace has fundamentally transformed every facet of our lives. It has the potential to revolutionise our future including our national security as contemporary global communication and connectivity are becoming increasingly dependent on cyber technologies. This dependency has exposed and increased the vulnerability of the cyber domain for its misuse for criminal activities, cybercrimes and cyber warfare, including cyber security threats or attacks against critical infrastructures. Knowing such potential misuse of cyberspace, states are ensuring the protection of cyberspace from cyber threats and cyber warfare to safeguard their social, economic and national security interests. States are introducing strong data protection laws and regulations to ensure secure access to such technologies, their application and the realisation of their true potential.

Pakistan has already embarked upon this path of digital transformation under the slogan "Digital Pakistan." Pakistan envisions "having a secure, robust and continually improving nationwide digital ecosystem ensuring accountable confidentiality, integrity and availability of digital assets leading to socio-economic development and national security." To materialise this digital transformation, Pakistan has taken several initiatives including drafting Pakistan's Cyber Security Policy 2021 and attaches top priority to securing Pakistan's cyberspace in its National Security Policy 2022-2026. However, there is a need to raise awareness, promote cyber security culture, bridge the technological divide, develop cyberspace norms and address other related challenges at the national level. This requires a comprehensive and result-oriented discussion among all relevant stakeholders.

Remarks by Dr Siraj Ahmed Shaikh, Coventry University, United Kingdom

Dr Siraj Ahmed Shaikh, Professor of Systems Security, Coventry University, UK, shared his views on "Ensuring Cyber Safety and Security of Critical Infrastructure." While talking about

the strong national security and a critical infrastructure perspective on many cyber-physical systems, he laid out the premise of the problem at hand. There are two fundamental differences when experts talk about cyber security. One is the computer system that is right in front of us. It is all the data and the code. These are traditional computers and traditional IT equipment networks in some way. It may have a security implication because of any malicious kind of manipulation but largely its impact is confined to either some data disclosure or some disruption.

The second part of this problem domain is the cyber-physical systems. These are usually safety-critical systems that have some physical manifestation so they could be smart home cameras. But more importantly critical infrastructure could be anything from transport infrastructure that could be maritime vessels that could be cars on the road health care infrastructure that could be hospitals connected for some critical surgery delivery and so on military systems that could be used for all kinds of defensive offensive kind of capabilities. For a nation-state and several other infrastructures that could be rather scoped into that. Therefore, the security of those traditionally somewhat safely critical systems is then a completely different subject that requires of course an understanding of the threat actor because any threat to that is posed by a very serious player usually with some state backing and some serious non-state backing. It also involves a deeper understanding of not just traditional computer science and networking but engineering electronics, control systems, communication systems and a number of those technologies that may be relevant to the domain itself. This makes the subject very complicated.

There are two things when it comes to developing and maturing capabilities for security and safety-critical systems. They are much-related domains but they are fundamentally different domains. Therefore, for any nation-state, the first thing we want to think about is where the risk ownership and the operational ownership for these sectors are. For example, if we were talking about smart home systems or even automotive systems then the private sector usually would have many standards of best practices and regulatory authority that would look at traditional safety issues to comply so the systems would comply with certain safety regimes. Increasingly, they would set up bodies where they share threats or they would regulate various compliance regimes and so on to make sure that products are complying with some safety requirements so

there are international standards.

In the context of Pakistan, how do we structure that kind of risk ownership and that sectoral ownership? It cannot be the one cyber body overlooking all of this, there may be which could facilitate but it needs sectoral knowledge. However, there are systemic risks that lie within those different sectors. The automotive industry has a different understanding of functional safety and road safety than the nuclear power industry would have. Therefore, there are different levels of maturity. It is important to think about whether the state takes ownership in the case of energy systems and whether the private industry takes ownership when it comes to automotive systems. Before getting into regulation that kind of structure is very important. It is also important to make sure of a healthy structure and ecosystem. Safety is a much more established regime in terms of knowledge, certifications and standards. How do typical mature economies address this? The role of local adoption of standards and best practices is very important. Global standards may be very useful but an automotive security standard will be implemented differently in Japan and Germany, very mature economies than in developing regions such as South Asia. Therefore, in the safety world experts have acknowledged a reference architecture.

Remarks by Dr Haider Abbas, NUST

Dr Haider Abbas, Director, National Cyber Security Auditing & Evaluation Lab, Military College of Signals (MCS) – NUST spoke on "National Information Security: Lessons for Pakistan." He highlighted the increasing dependency of states on cybersecurity. He said that we are living in an era where most of the critical infrastructures are dependent on cybersecurity in which a big number of wired and wireless devices are making things extremely complex. The emerging critical threats in the cyber domain are going to affect the economy of a state. Cyberwarfare combined with electronic warfare becomes even more dangerous for nation-states.

While talking about the major categories of cyberattacks against Pakistan, he said that they could be divided into three categories: against people, against organisations and against the government. Due to the recent Pegasus attack that compromised several devices, there is a potential risk that critical information has been leaked. Dr Haider also mentioned recent

cyberattacks on the Careem and the FBI websites by Indian hackers. The cyber threat landscape of Pakistan shows that these attacks affected people at all levels. One of the major reasons behind these successful attacks is the state's huge reliance on third parties rather than on initiating national cyber security initiatives at a different level. The official data is being compromised due to weak cyber security mechanisms followed by the public sector organisations without any risk assessment mechanism. Additionally, the common use of pirated software and the same password by multiple users increases the security risks. Despite PTA's restrictions, banned sites are still accessible through different software. Furthermore, there is a general careless attitude in people vis-a-vis data.

There is a need to raise awareness about cybersecurity to ensure good cyber hygiene. Moreover, there is a need to develop technical solutions and make them available at the organisational and individual levels. Every organisation must formulate its cybersecurity policy, perform a risk assessment of the organisation to figure out its vulnerabilities, install firewalls and anti-virus on their personal as well as official devices and use multi-factor authentication. Other measures include the establishment of national and development of indigenous tools to facilitate audit and compliance mechanisms, introduce indigenous software and trained human resources to ensure the physical protection of cyberinfrastructure and establish national and sectorial CERTS for rapid crisis management.

Professor Dr Khashif Kifayat, Director NCC, Air University, Islamabad

Professor Dr Khashif Kifayat, Director, National Centre for Cybersecurity, Air University, Islamabad presented his views on "Building National Cyber Disaster Recovery Model and Challenges for Pakistan." He said that cyber security is not Pakistan's problem only but it is a transnational phenomenon. Globally these attacks from malicious actors affect people. Pakistan is highly motivated to protect its critical assets and the public. To achieve that goal, Pakistan has introduced its National Security Policy and the National Cybersecurity Policy. If Pakistan is motivated to eradicate cybersecurity issues, then it should develop a technical as well as a non-technical skill set.

From the technical side, many public sector organisations are unaware of the actual magnitude of the cyber threat and data loss due to a lack of information and cyber security awareness. To

enhance the speed and quality of response, the government should first identify the critical assets and perform a comprehensive risk assessment. A heavy loss could be avoided by establishing a multi-layered defence mechanism and making the organisation aware of it. Most of the time, a cyberattack is not just about one-time damage, it's about critical data theft that could be misused for several diverse attacks with serious consequences in future. On the non-technical side, the government should initiate proper alertness that includes a massive awareness campaign, especially in educational institutes. A human being is an asset that lies at the core of cyberspace. Therefore, the state should also work on building the technical capacity of the public to defend themselves from malicious attacks. The state should make data protection measures mandatory for every organisation operating in Pakistan. The state should also make sure that everyone must be aware of cybersecurity from the top executives to lower employees.

Ms Aamna Rafiq, Research Associate ACDC-ISSI

Ms Aamna Rafiq, Research Associate, Arms Control & Disarmament Centre (ACDC) -ISSI made a presentation on "Creating National Cyber Security Culture in Pakistan." she said that cybersecurity culture is not a properly defined concept due to a difference in the understanding about what demarcates a cybersecurity culture. Academic and industrial research has led to the development of a clearer definition of what a cybersecurity culture is. "Cybersecurity culture is the human behaviour that protects organisational information through compliance with the organisation's security policies and procedures and an understanding of how to execute them as embedded through initiatives such as training, education, awareness and communication." Cybersecurity culture could also be described as a way that things are done. It consists of secure behaviours that have become habitual and require less cognitive effort. It is also known to be an effective tool that helps manage the human factors within cybersecurity because employee individual is known to either create or reduce vulnerabilities.

While highlighting the significance of cybersecurity culture, she said that managing cyber defences only through borrowed tactics from the annals of traditional warfare, with an increasing emphasis on securing all boundaries and delivering a knockout is no longer effective. In the contemporary interconnected world, digital boundaries are becoming more and more porous. Furthermore, the civilian roles of cyber technologies are expanding. A growing number of

essential business functions are being performed online. However, the nature of cybercrime is also maturating and mutating. The increasingly sophisticated cyberattacks require a coordinated team effort based on the principle of shared responsibilities.

The security culture of the state has its specific dynamics and boundaries that decide what can be securitised. The national security culture is securitised at a general level in such a way that any new security issue automatically moves to the already securitised area of traditional security. In Pakistan, cybersecurity operated in the absence of relevant institutions or under the domination of the institutions established because of other types of securitisations. Furthermore, there is an absence of resonance between the public and national cybersecurity narrative. Presenting something like an existential threat to cybersecurity does not necessarily result in securitisation. Pakistan should focus on building credible voices of cybersecurity for a resolute acceptance of cybersecurity policy, laws and culture. She also recommended measures to be taken in political, economic, legal, management, and monitoring domains

Table 1: Approaches and Measures to Strengthen Cybersecurity Culture in Pakistan

Type of Approach	**Recommended Measures**
Political	• Start a National Awareness Campaign • Establish a Dedicated Body for Cybersecurity Culture • Allocate Dedicated Financial Capital • Design National Cybersecurity Curriculum • National Capacity Development Programme
Legal	• Draft Cybersecurity Policy, Strategy and Doctrine

	• Develop Cybersecurity Standards • Adopt Industry Competency Models • Establish Compliance Accreditations
Management	• Establish Cybercrime Units in Local Police Stations • Establish Specialised Cybercrime Courts • Establish Cybersecurity Inspection Programme
Monitoring	• Define Benchmarks • Define Success Indicators for Initiatives • Develop Acceptable Practices • Publish Periodic Process Reports
Economic	• Develop Stakeholder Engagement Plan • Promote Public-Private Partnerships • Design Cybersecurity Research Agenda – Increase Knowledge base • Increase International Partnerships

Concluding Remarks by Ambassador Aizaz Ahmad Chaudhry, Director-General, ISSI

While emphasising the importance of international legal infrastructure, Ambassador Aizaz Ahmad Chaudhry, Director General ISSI, said that there is a great deal of effort being made by Pakistan to develop legislation at the national level to prevent the misuse of cyberspace or

regulate it for creating incentives for good uses. However, at the international level, there is a reluctance on the part of those who already have an advantage in the cyber domain to create an international legislative structure. In the absence of an international legal structure, every state is operating from a self-help approach. There is a need to make a move for an international legal regime for cyberspace.

PICTURES OF THE EVENT