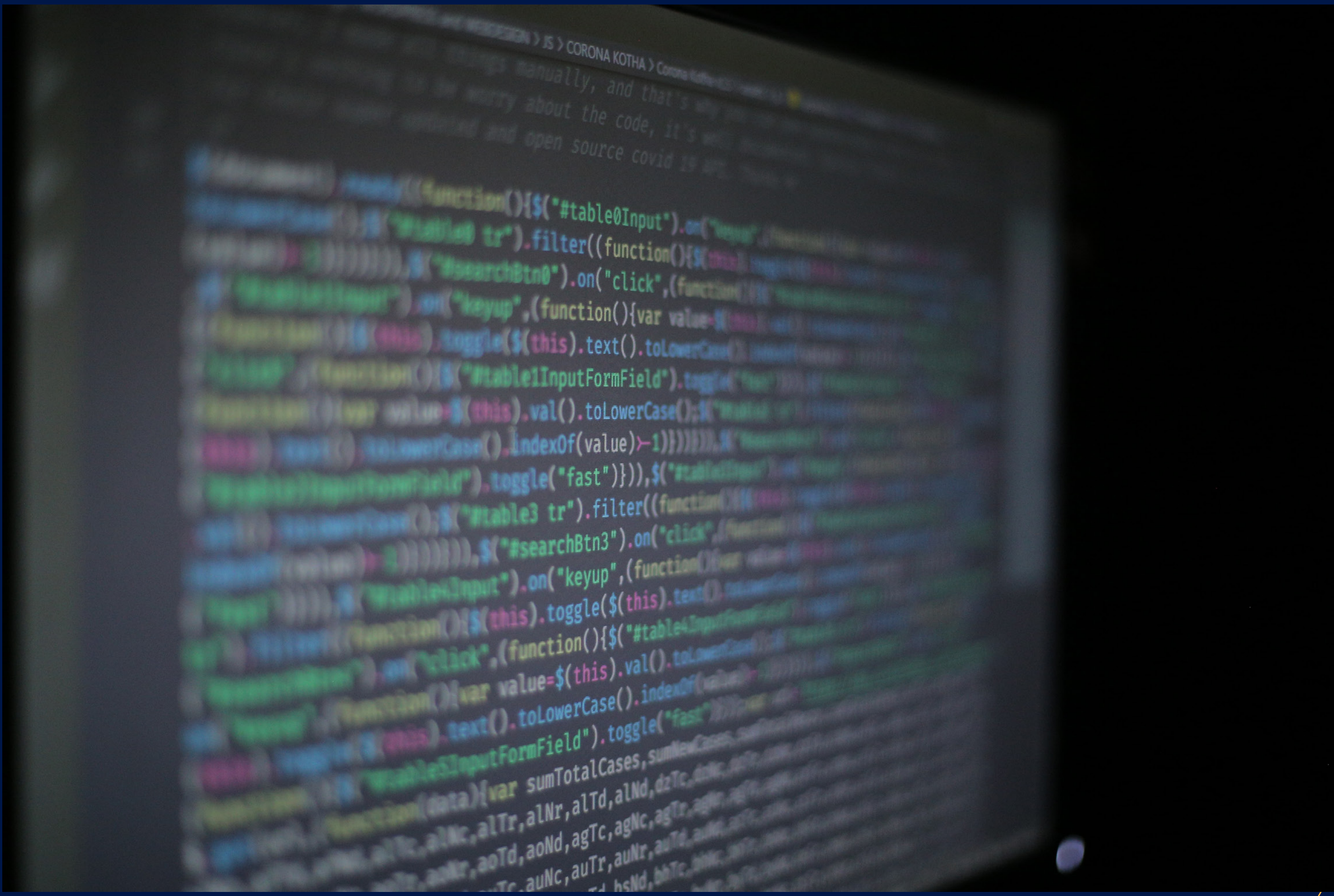
DCAF Geneva Centre for Security Sector Governance



Cybersecurity Governance in South Asia

Thematic SSG Brief

Rohit Karki, Justin Yu, ASM Ali Ashraf, Bart Hogeveen, Ammar Jaffri, P K Mallick, Francesca Spidalieri, and Harinda Vidanage

ASIA-PACIFIC SECURITY SECTOR GOVERNANCE NETWORK

DCAF Geneva Centre for Security Sector Governance

Published in Switzerland by DCAF - Geneva Centre for Security Sector Governance
Maison de la Paix, Chemin Eugène-Rigot 2E
CH-1202 Geneva, Switzerland
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva

First published in March 2023.

Cite as: Rohit Karki, Justin Yu, ASM Ali Ashraf, Bart Hogeveen, Ammar Jaffri, P K Mallick, Francesca Spidalieri, and Harinda Vidanage. Cybersecurity Governance in South Asia. Thematic SSG Brief. Geneva: DCAF - Geneva Centre for Security Sector Governance, 2023.
Series editor: Albrecht Schnabel
ISBN: 978-92-9222-691-6
Cover picture: Cover art by Dhaka-based photographer Al Nahian, freely accessible through Pexels.com.

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity-building of both state and non-state security sector stakeholders

Disclaimer

The opinions expressed in this publication are those of the authors alone and do not necessarily reflect the position of the institutions referred to or represented within this publication.

Additional resources

The workshop programme and links to recordings of the public webinar are available at https://www.asiapacificssg.com/post/public-webinar-cybersecurity-governance-in-south-asia.

Acknowledgements

The authors would like to thank DCAF's SSG Associates of the South Asia Security Sector Governance Network for proposing the topic of this thematic brief, participating in the preparation of the expert workshop on which the brief is based, providing their invaluable support in identifying the regional experts involved in the project, and contributing their own unique perspectives to the brief. As is the case for all activities by DCAF's Asia-Pacific Unit, the contributions of the SSG Associates Aftab Nabi, A. N. M. Muniruzzaman, Indika Perera, and Roshan Khaniejo, were very helpful for planning the workshop, and for providing support on the production of the thematic brief.

We are also very grateful to our fellow colleagues for supporting the planning process of the workshop and contributing their valuable insights to this brief, and for their patience in responding to our requests for revisions and updates during the brief's preparation.

Special thanks are also due to the series editor of the SSG Thematic Briefs, Albrecht Schnabel, who provided overall supervision and guidance to the brief's authors.

Finally, we thank Sabeena Bali for copyediting and proofreading and Floris de Klerk Wolters for preparing the final layout.

Executive Summary

In South Asia, there has been a growing recognition of new types of threats emerging in cyberspace. These threats include the misuse of digital technologies for malicious purposes, such as military cyber operations, cybercrime, disruptions of essential services, violations of privacy, data exploitation, surveillance, disinformation, cyberespionage and cyberterrorism. Governing cyberspace and establishing a common set of rules to address these issues pose several challenges for policymakers in South Asia. These diverse challenges range from inter-state challenges that are due to rivalries, distrust and a tense geostrategic environment, to intra-state challenges that relate to internal politics and budgetary considerations. They present significant obstacles to reaching a regional or even national consensus on cybersecurity governance. This brief highlights the links between cybersecurity and the concept of good security sector governance (SSG), paying particular attention to the relevant principles, actors and challenges. It then discusses the specific cyberthreat landscape of South Asia, focusing on two recent major cyberattack incidents — the Bangladesh Bank heist and the hacking of Mumbai's power grid. The brief also sheds light on the important role of the UN Norms of Responsible State Behaviour in Cyberspace and discusses the Norms' relevance in the South Asian context. Additionally, it highlights the development and implementation of national cybersecurity strategies and their relevance for improving cybersecurity governance in South Asia. Finally, a set of recommendations for promoting good SSG in cyberspace is provided. These recommendations include integrating international standards, such as the UN Norms of Responsible State Behaviour in Cyberspace, into government policy and legislation, organising cybersecurity awareness campaigns to better communicate risks and concerns related to cybersecurity and to promote best practices in cyber hygiene, and promoting regional initiatives to exchange best practices and lessons learned regarding good SSG in cybersecurity in different South Asian states.

Table of Contents

Introduction

Over the last decade, countries around the world have embarked on a digital transformation journey embracing and embedding information and communications technologies (ICTs) into their networked environments and infrastructures to improve productivity, efficiency, innovation and competitiveness. In particular, South Asian countries have prioritised digitisation and connectivity to foster economic growth, enable skills development, encourage modernisation, and advance human and social development, and as a means to accelerate the achievement of the UN Sustainable Development Goals (SDGs), which all have digital dimensions. However, their rapid digitisation – often underpinned by insecure ICT infrastructure, legacy software and vulnerable devices – has introduced new risks and vulnerabilities and exposed them to significant cyber harm, which in turn is threatening the security and resilience of their digital infrastructure and systems and eroding trust in the digital environment.[1]

These threats are why cybersecurity must be considered a national and international development and security priority, which both state and non-state actors across the globe are increasingly forced to grapple with. Cyber threats can span from cyber-criminals using ransomware against businesses and critical services (e.g., hospitals, schools and municipalities) to state-sponsored malicious actors seeking access to sensitive information, to non-state groups using cyberspace as a conduit for radicalisation. While there is a need to increase the capacity and capabilities of state and non-state actors to defend against such cyber threats, there is also a need to adhere to good governance principles to safeguard the digital development process from associated risks, challenges and disruptions. An over-securitisation of cyberspace in pursuit of absolute cybersecurity would be impossible and would undoubtedly infringe upon fundamental freedoms and civil liberties that are indispensable to democratic societies.

In addition to the importance of tackling cyber threats and balancing cybersecurity needs with good governance principles, there is a need to address cybersecurity governance challenges arising from a number of other factors. Firstly, cyberspace presents several challenges to democratic oversight. These include the intrinsic complexities of cyberspace that make enforcement of the rule of law and attribution of cyber attacks difficult, the technical capabilities required for effective regulation, the inherent dual-use nature of cyber tools[2] and the wide range of actors involved in governing cyberspace, including non-state entities.[3]

Secondly, international frameworks on cyber governance are not yet widely agreed upon and remain contested. The main efforts by nation states to agree on a set of international standards for the governance of cyberspace in the context of inter-state relations include the United Nations Group of Governmental Experts on Information Security (UNGGE) and the UN Open-Ended Working Group (OEWG), which has succeeded in establishing 11 voluntary and non-binding norms of responsible state behaviour in cyberspace. These norms govern what states can and cannot do in cyberspace during peacetime and are supposed to inform and guide the application of international law in cyberspace. This set of norms is intended to enhance security and prevent conflicts, which is important to preserve a free, open, secure and peaceful cyberspace. Other international bodies, such as the International Telecommunication Union (ITU), contribute to the formulation and implementation of international standards on ICTs and cybersecurity by developing models and frameworks for governing cyberspace and assessing national cyber maturity.

Governing cyberspace and establishing a common set of rules in South Asia presents several challenges for policymakers. These challenges range from inter-state challenges due to rivalries, distrust and a tense geostrategic environment, to intra-state challenges relating to internal politics and budgetary considerations. They present significant obstacles to reaching international and even national consensuses on cybersecurity governance. However, effective cybersecurity governance and good practices in the region are sorely needed in light of cyber-enabled campaigns such as the Bangladesh Bank Heist in 2016[4] and the disruption of Mumbai's power grid in 2020[5].

This Thematic Security Sector Governance (SSG) Brief begins by exploring the linkages between cybersecurity and the concept of good SSG, considering relevant principles, actors and challenges. It then discusses the specific cyber threat landscape of South Asia, drawing upon the two major cyberattack incidents— the Bangladesh Bank heist and the hacking of Mumbai's power grid. Finally, it presents the aforementioned 11 UN norms of responsible state behaviour in cyberspace as well as examples of national cybersecurity strategies, applying them to the South Asian context.

Linkages Between Cybersecurity and Security Sector Governance

SSG is a lens that is rarely applied to the issue of cybersecurity. However, there are many ways in which an SSG-driven approach can contribute to improving the effectiveness of governance and accountability of cybersecurity stakeholders. This includes incorporating an understanding of human security into cybersecurity, such as the recognition that individuals and communities have different specific security needs, including in cyberspace. This section will elaborate on how the concept of good SSG can be linked to the issue of cybersecurity through an understanding of the principles of good governance, the roles of different actors in ensuring these principles and the unique obstacles that cyberspace presents to ensuring good SSG.

[1] M. Hathaway and F. Spidalieri (2021) "Integrating Cyber Capacity into the Development Agenda", *Global Forum on Cyber Expertise*, thegfce.org/wp-content/uploads/2021/11/Integrating-Cybersecurity-into-Digital-Development_compressed.pdf.

[2] The same technology can be used for both legitimate and malicious purposes, or in relation to military operations, for both offensive and defensive purposes.

[3] DCAF – Geneva Centre for Security Sector Governance (2021) "Guide to Good Governance in Cybersecurity", 19 January, pp. 13-14, .

[4] K. Zetter (2016) "That Insane, $81M Bangladesh Bank Heist? Here's What We Know", *The Wired*, 17 May, .

[5] K. Bommakanti (2021) "China's cyberattack on Maharashtra power grid was to improve PLA's bargaining position", *The Print*, 12 March, theprint.in/opinion/chinas-cyberattack-on-maharashtra-power-grid-was-to-improve-plas-bargaining-position/620274/.

Key Concepts[6]

Good Security Sector Governance (SSG) describes how the principles of good governance apply to public security provision, management and oversight. The principles of good SSG are accountability, transparency, the rule of law, participation, responsiveness, effectiveness and efficiency. Establishing good SSG is the goal of SSR.

Security Sector Reform (SSR) is the political and technical process of improving state and human security by making security provision, management and oversight more effective and accountable within a framework of democratic civilian control, the rule of law and respect for human rights. SSR may focus on only one part of public security provision or the way the entire system functions, as long as the goal is always to improve both effectiveness and accountability.

The security sector is not just security providers; it also includes all the institutions and personnel responsible for security management and oversight at both national and local levels.

For more information on these core definitions, please refer to the DCAF's SSR Backgrounders on 'Security Sector Governance', 'Security Sector Reform' and 'The Security Sector'.
DCAF — Geneva Centre for Security Sector Governance, 'Security Sector Governance', SSR Backgrounder Series, 2015, https://www.dcaf.ch/security-sector-governance-applying-principles-good-governance-security-sector-0.
DCAF — Geneva Centre for Security Sector Governance, 'Security Sector Reform', SSR Backgrounder Series, 2015, https://www.dcaf.ch/security-sector-reform-applying-principles-good-governance-security-sector-0.
DCAF — Geneva Centre for Security Sector Governance, 'The Security Sector', SSR Backgrounder Series, 2015, https://www.dcaf.ch/security-sector-roles-and-responsibilities-security-provision-management-and-oversight.

At its core, linking cybersecurity and SSG requires an application of the principles of good governance to cybersecurity provision, management and oversight. These principles include accountability, transparency, rule of law, participation, responsiveness, effectiveness and efficiency. Applying these principles to cybersecurity governance, or in other words cybersecurity provision, management and oversight over cybersecurity providers, requires adapting them to the specific context of cyberspace. For example, given the importance of non-state actors in cyberspace, ensuring accountability in cybersecurity provision and management requires oversight actors to monitor the contributions of state and non-state actors to cybersecurity. Applying the rule of law requires a new approach to regulatory frameworks, which can be evidenced by the development of comprehensive national cybersecurity strategies. To improve the effectiveness of cybersecurity provision, measures such as the creation and development of computer emergency response teams (CERTs) are required.

In applying these principles, different actors play important cybersecurity provision, management and oversight roles. Security providers such as CERTs, national cybersecurity agencies, specialised units of the armed forces, intelligence agencies, law enforcement and vendors of cybersecurity software all play an important role in providing cybersecurity by preventing, responding to, mitigating and investigating cyber attacks, cyberespionage and cybercrime. Governments are responsible for establishing an overarching national cybersecurity architecture, typically laid out in dedicated national cybersecurity strategies. In the case of cybersecurity, the private sector is also responsible for management by formulating and enforcing community standards. The legislative branch of government (e.g., parliament) is often tasked with cybersecurity management and oversight roles, taking into account the specific risks and challenges faced by the country in cyberspace. Their responsibility to approve relevant and appropriate cybersecurity legislation, among other things, should not compromise fundamental human rights. Non-state oversight actors, such as civil society and the private sector, similarly play an important role in strengthening the cybersecurity of a country.

These actors face a number of obstacles in applying the principles of good governance to cybersecurity that result from the unique governance challenges posed by the complexity of cyberspace. One such challenge is the technical complexity of online networks, which makes it difficult for oversight bodies like parliamentary committees to perform their oversight role. This is compounded by legal complexities such as jurisdiction and how to adapt legal frameworks to the context of cyberspace. While cyberspace's physical infrastructure may be contained within state boundaries, the transnational flow of data and information complicates questions of jurisdiction and authority. There are also challenges to the implementation of international and regional cybersecurity norms and standards at the national level, such as balancing the need to adhere to recognised international human rights norms with national security concerns. Finally, while cooperation between the public and private sectors is fundamental to the effective governance of cyberspace, it is also increasingly difficult due to the lack of clarity around roles and responsibilities as well as mistrust and other barriers to the sharing of timely and relevant information.

The issue of trust is a key obstacle to the effective governance of cyberspace. Close cooperation between state and non-state actors is essential to strengthening cybersecurity, but the ambiguity of malicious activity in cyberspace leads to a lack of information, an inability to verify specific claims and the ineffectiveness of direct state control. Given this complex landscape, identifying responsible actors (i.e., states) that can be held accountable for malicious activity in cyberspace is fundamental. This point will be explored further in relation to the UN norms on responsible state behaviour in cyberspace and the development of national cybersecurity strategies, both of which can help overcome the issues of trust and confidence in the digital environment.

Overall, applying the concept of good SSG to cybersecurity is no simple task. It is nonetheless essential to facilitate governance of cyberspace that balances the need to protect sensitive information, critical infrastructures and so on with the need to safeguard the fundamental rights of individuals and communities. In adopting an SSG lens to view cybersecurity, it is important to understand the diverse range of actors involved

[6] The definition of these key concepts is taken from DCAF's SSG Backgrounder series.

in cyberspace, evaluate who controls which areas of cyberspace and consider how to incentivise adherence to the principles of good SSG. It is also important to evaluate how the principles of SSG can be best applied to specific contexts, which includes considering the most relevant cybersecurity threats in a given country and/or sector.

Emerging Cybersecurity Threats in South Asia

Cyberthreats and the misuse of digital technologies for nefarious purposes include military cyber operations, cybercrime, disruptions of essential services, violation of privacy, data exploitation, surveillance, disinformation, cyberespionage and cyberterrorism.

This section discusses the specific cyber-related threats that states and societies in South Asia are facing, including trends that South Asian security experts have identified as the most relevant and concerning in their respective countries. These trends include the evolving dynamics of geopolitical rivalries, increasing vulnerability to cybercrime as a result of rapid digitalisation which has been accelerated by the COVID-19 pandemic and the misuse of cyberspace and digital technologies either by terrorists for recruitment and communication or by individuals spreading mis- and disinformation. The latter, while not a direct challenge to cybersecurity, runs contrary to the good governance of cyberspace. Ironically, it depends on the trust and confidence in communicating through cyberspace that cybersecurity provides. Finally, two specific examples of cyber intrusions – the attack on Mumbai's power grid and the Bangladesh Bank Heist – will be discussed.

The geopolitical context of South Asia has been fraught for decades and the region is not unfamiliar with inter-state conflict. However, the proliferation of cyber tools as part of the national security toolbox of most developed countries (in order to project power, influence global politics, impose their interests, and/or conduct cyber operations in and through cyberspace) has added an additional sphere of potential confrontation between states and exacerbated the risk of misperception and miscommunication. This introduces cybersecurity challenges not just for regional powers engaged in competition but also for the many small states in South Asia that do not wish to take sides between larger cyber powers or become sites of confrontation or competition. An increase in the use of cyber technologies as part of geopolitical confrontation has the potential to cause unforeseen consequences and impact relations between South Asian countries. These consequences highlight the importance of considering the spillover effects of cyber capabilities and ensuring accurate attribution of cyberattacks.

The digitalisation of South Asian societies is another trend that increases the need for effective cybersecurity. Initiatives such as Digital India and Digital Pakistan in South Asia are representative of the drive by governments and businesses in the region to incorporate digital technologies into every layer of South Asian society. Aside from this deliberate top-down push for digitalisation, there is also a clear societal shift towards connectivity in South Asian states. For example, the internet penetration rate in India increased from 27 percent in 2015 to 47 percent in just six years.[7] This trend towards digitalisation is further compounded by the increased dependence on digital technologies that has resulted from the COVID-19 pandemic. This rapid digitalisation prioritised preserving connectivity rather than addressing security vulnerabilities. Indeed, the uptake of digital technologies and internet connectivity has not been accompanied by adequate investments into cybersecurity. This has exposed these countries to greater security vulnerabilities and malicious activities that are threatening the security and resilience of their digital infrastructure and systems and eroding trust in the digital environment.

Furthermore, the COVID-19 pandemic has exacerbated another worrying trend in South Asia and elsewhere, namely the misuse of cyberspace to spread mis- and disinformation. In countries with Muslim minorities such as India, Sri Lanka and Nepal, the internet has been used to propagate Islamophobic sentiments, contributing to and playing off of existing intercommunal tensions.[8] Social harmony has also been threatened in religiously diverse Bangladesh, with disinformation on social media stoking sectarian violence. This misuse of the internet and social media platforms to spread disinformation has followed the use of the internet by terrorist groups for propaganda as well as internal communication. In Sri Lanka, for example, terrorism has become more of a security concern including in terms of cybersecurity following the Easter Sunday bombings of 2019, an attack that shocked a country unfamiliar with radical Islamist terrorism and spurred the drafting of a stringent cybersecurity bill.

Two incidents, in particular, help demonstrate the relevance of these trends and the cybersecurity needs facing South Asian countries. The first is the attack on the Mumbai power grid in 2020. The attack occurred four months after a violent clash between Chinese and Indian troops in the Galwan Valley. Some believed the attack was directly connected to the confrontation.[9] A study by Recorded Future found that malware from a Chinese state-sponsored group named Red Echo was used to infect India's electricity grid at the time of the border clash, although the study did not draw a conclusion on the link between this malware and the subsequent power outage.[10] Indian officials have been hesitant to explicitly blame the Chinese government or military for the power outage, pointing to the difficulties in assigning responsibility for cyber attacks to another state. However, Nitin Raut – then Energy Minister of Maharashtra state in which Mumbai is located – did call the power grid failure a cyber attack and an act of sabotage. This incident, if indeed related to the territorial dispute between China and India, demonstrates the evolution of traditional geopolitical rivalries in the region with the addition of a cyber dimension. It also demonstrates the vulnerability of critical infrastructure, with this attack striking at a

[7] T. Basuroy (2022) "Internet penetration rate in India from 2007 to 2021", *Statista*, 9 June, www.statista.com/statistics/792074/india-internet-penetration-rate/.

[8] K. Yadav, I. Thange, J. Ilhardt, S. Siwakoti and J.N. Shapiro (2020) "Old hatreds fuel online misinformation about COVID-19 in South Asia", *Bulletin of the Atomic Scientists*, 25 November, thebulletin.org/2020/11/old-hatreds-fuel-online-misinformation-about-covid-19-in-south-asia/.

[9] D.E. Sanger and E. Schmall (2021) "China Appears to Warn India: Push too Hard and the Lights Could Go Out", *The New York Times*, 28 February, www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html.

[10] Insikt Group (2021) "China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions", *Recorded Future*, 28 February, www.recordedfuture.com/redecho-targeting-indian-power-sector.

time of particular vulnerability as a large part of the Indian population had transitioned to working from home amid the COVID-19 pandemic.

A previous case also demonstrates the vulnerability of South Asian states to large-scale cybercrime. The 2016 heist of the Bangladesh Central Bank resulted in the theft of US$81 million from the bank, although hackers even intended to steal US$1 billion.[11] The heist involved a complex operation that exploited the SWIFT credentials of Bangladesh Central Bank employees to request authorisation from the Federal Reserve Bank of New York to transfer the funds from the Bangladesh Bank to a number of Asian banks. The malware used in the attack was similar to the Sony hack attributed by the US to North Korea, leading some to believe North Korea was behind the heist, although to date this has not been confirmed. The heist highlighted the need for robust cybersecurity practices and pointed to the vulnerability of SWIFT, a system that is essential to international banking. Since the heist, Bangladesh has put more emphasis on cybersecurity and is now ranked 11th out of 38 Asia-Pacific countries in cybersecurity maturity, according to the ITU's Global Cybersecurity Index.[12]

The Importance of UN Global Norms on Responsible State Behaviour in Cyberspace

Threats to the security and stability of cyberspace have been recognised by the international community as priorities demanding common agreements on potential mitigation strategies and responses. Over the course of more than a decade, UN member states built the UN Framework for Responsible State Behaviour in Cyberspace to manage the increasing scope, scale, severity and sophistication of cyber threats. This framework includes a recognition that international law applies in cyberspace, norms of responsible behaviour, the development of confidence-building measures and a commitment to increasing capacity-building efforts. The most well-known and actionable part of the framework is the 11 UN norms of responsible state behaviour in cyberspace.

The 11 norms are composed of eight steps that states should take and three that states should avoid. Importantly, they seek to overcome some of the aforementioned governance challenges that cyberspace poses. For example, norm 3 prescribes that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs, seeking to clarify the jurisdictional challenges that operations in cyberspace present. Similarly, norm 2 directs states to consider all relevant information before assigning responsibility for cyber attacks and is therefore related to the challenges that malicious cyber activities pose in terms of attribution.

Implementation of these norms involves progressing along an implementation tree of several steps, which include awareness, recognition, assessment, understanding, planning and acting, and implementation. Progressing along this tree would also involve demonstrating implementation, for example by expressing political commitments, integrating norms into legal frameworks and official documents, and actively building cyber capabilities.[13]

However, reconciling the theory and practice of norm implementation can be a challenging task. In South Asia in particular, there are clear obstacles to harmonising and promoting compliance with the 11 UN norms. The India-Pakistan rivalry, for example, as well as the prioritisation of national security interests and national sovereignty mean that interstate cooperation on cybersecurity – the very first of the 11 norms – remains difficult. The challenges to effective interstate cooperation on cybersecurity in South Asia is demonstrated by the lack of progress in regional initiatives on cybersecurity within regional bodies such as the South Asian Association for Regional Cooperation (SAARC) and the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC). The 2014 SAARC Summit, for instance, saw an agreement to establish a cybercrime monitoring desk but no significant progress has been achieved since then. Similarly, there has been no progress in establishing a joint forum for cybersecurity within BIMSTEC.

These difficulties, however, do not preclude the 11 norms from serving as useful topics of discussion and cross-regional interaction among non-state entities such as think tanks, the cybersecurity industry and civil society organisations. The 11 norms also remain the best existing framework for state and non-state actors to hold other states accountable for their violations. Despite a lack of enforcement power, the norms offer the clearest current means to assess whether the behaviour of a state violates agreed norms and should be considered unacceptable behaviour. The norms also form an integral part of improving SSG in cyberspace at both international and national levels. For instance, the norms recommend that states clarify ambiguities in institutional responsibility that obstruct the application of the principles of good SSG to cybersecurity, provide guidance for the protection of critical infrastructure and ICT supply chains, encourage joint efforts to tackle cybersecurity threats, and respect the impartial character of national CERTs. One way in which these norms can contribute to good SSG in the cybersecurity context is through their incorporation into national cybersecurity strategies, as is the case in the latest iteration of Bangladesh's National Cybersecurity Strategy.

National Cybersecurity Strategies

The development and implementation of national cybersecurity strategies (NCSs) is a key component of good SSG in cybersecurity. They represent the single clearest way for governments to establish a unified, whole-of-government approach to cybersecurity governance by outlining the vision, high-level objectives, institutional responsibilities and priorities to guide the country in addressing cybersecurity in alignment with their

[11] K. Zetter (2016) "That Insane, $81M Bangladesh Bank Heist? Here's What We Know", *Wired*, 17 May, www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/.

[12] International Telecommunication Union (2021) "Global Cybersecurity Index 2020", p. 29, www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

[13] B. Hogeveen (2022) "The UN norms of responsible state behaviour in cyberspace. Guidance on implementation for Member States of ASEAN", *Australian Strategic Policy Institute*, www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace.

national security and economic priorities. They also lay out the steps, programmes and initiatives that a country will undertake to protect its critical infrastructure and increase its security and resilience, as well as allocate human and financial resources. The process of developing national cybersecurity strategies does not occur within a vacuum, as there is a wealth of experience that countries around the world have gained from their own efforts in developing NCSs. These strategies can take many forms and can go into varying levels of detail, depending on the particular country's objectives, priorities, specific needs and levels of cyber-readiness. Organisations such as the ITU and DCAF as well as the Global Forum on Cyber Expertise have been collecting different examples and specific experiences of countries that have published NCSs that can provide guidance to other governments seeking to develop new strategies or update older ones.

The ITU, together with a consortium of 18 other organisations with demonstrated and diverse experience in the cybersecurity field, including IGOs, MDBs, the private sector and academia, published the first 'Guide to Developing a National Cybersecurity Strategy', which offers the most comprehensive – and yet fairly easily employable – framework to develop and implement comprehensive, inclusive and sustainable NCSs that take into consideration a country's specific socio-economic vision, political context, and cultural and societal values and encourage the pursuit of secure, safe and resilient digital societies.[14] This framework provides a flexible roadmap to support national leaders and policymakers in their ongoing effort to develop, update, implement, monitor and evaluate NCSs, including cyber-preparedness and digital resilience. The NCS Guide details the five key steps in the development of a NCS from preparation to drafting, publication, implementation, monitoring and evaluation, and a set of good practice elements under seven focus areas that can make a strategy comprehensive and effective, while allowing for tailoring to the national context. The Guide also includes nine cross-cutting, overarching principles, applicable to all key focus areas, that should be considered in all steps of the strategy development process and that closely align with the principles of good SSG. These include a clear whole-of-government and whole-of-society vision; a comprehensive approach and tailored priorities; inclusiveness through the participation of all relevant stakeholders; the pursuit of economic and social prosperity; fundamental human rights; risk management and resilience; an appropriate set of policy instruments; clear leadership, roles, and resource allocation; and a trusted digital environment.

The DCAF 'Guide to Good Governance in Cybersecurity' also lays out a number of good practices that can help inform the development of NCSs.[15] These include, among others, integrating national strategies into broader national security policies, identifying a responsible authority, involving a broad range of relevant stakeholders and accompanying the strategy with an implementation plan. Another good practice entails the inclusion of additional strategic priorities: enhanced government coordination, reinforced public-private cooperation, improved international cooperation, and respect for fundamental human rights. Adhering to these good practices and the nine overarching principles of the 'Guide to Developing a National Cybersecurity Strategy', especially the allocation of clear leadership, roles and resources, can help NCSs evolve from simple documents to key pathways in achieving good SSG in cybersecurity.

These guidelines and frameworks for the development of comprehensive and effective NCSs are relevant to the South Asian context given the ongoing efforts to develop and improve national strategies in the region. India and Nepal, for example, are considering new strategies to update existing cybersecurity policies (their respective NCSs have yet to be published), while the Maldives still lacks such a strategy or policy. It is also important to note that drafting an NCS is only the first step in the lifecycle of a national cybersecurity strategy. The 'Guide to Developing a National Cybersecurity Strategy' identifies implementation and a formal process of monitoring and evaluation as phases IV and V of this lifecycle, and as such even South Asian states that have drafted an updated NCS need to ensure that the priorities identified in their strategies are translated into meaningful improvements in SSG.

Conclusion and Recommendations

This brief has explored how to apply a SSG lens to the cybersecurity context through the application of the principles of accountability, transparency, rule of law, participation, responsiveness, effectiveness and efficiency. It has justified the need for a tailored approach to applying these principles due to the particular challenges posed by governing cyberspace. These challenges include technical and legal complexity, as well as a need for international and public-private cooperation.

Using the principles of good SSG and having an appreciation of the roles and responsibilities of different actors within the security sector in South Asia are necessary to address the specific cyber threats faced by countries in the region, ranging from high-profile incidents like the Bangladesh Bank Heist and the Mumbai power grid failure to more frequent, low-level cases of cybercrime. Tackling these threats and vulnerabilities calls for significant improvements in the cybersecurity posture of South Asian countries, including the adoption of effective and efficient security provision without compromising the rights of individuals and communities.

The 11 UN norms and international guidance on the development of NCSs can facilitate the achievement of good SSG in cybersecurity. These frameworks provide foundational concepts which states can adapt to fit their own contexts while at the same time drawing upon internationally agreed-upon standards and the experiences of states that have reached a relatively higher level of cyber maturity.

While recognising the general progress made by South Asian states in the realm of cybersecurity in recent years, this progress varies from country to country and, even in

[14] International Telecommunication Union (2021) "Guide to Developing a National Cybersecurity Strategy – 2nd Edition", www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf.

[15] DCAF – Geneva Centre for Security Sector Governance (2021) "Guide to Good Governance in Cybersecurity", 19 January, pp. 68-77, www.dcaf.ch/guide-good-governance-cybersecurity.

the more successful cases, gains need to be consolidated and further strengthened in the long term. Effectively harmonising national legal frameworks in line with UN norms and developing NCSs are among the most important steps in improving the governance of cyberspace in South Asia, to clarify jurisdiction and mandates, allocate necessary resources to build and foster local cybersecurity expertise, and ensure buy-in from a wide range of stakeholders involved in strengthening cybersecurity.

With all of this in mind, there are a number of possible actions that South Asian states could take in their efforts to achieve good SSG in cybersecurity. Firstly, international standards such as the UN norms of responsible state behaviour in cyberspace should be integrated into government policy and legislation. Not only would applying these standards help bring the governance of cyberspace in line with the principles of good SSG, but they would also demonstrate a willingness to follow and apply internationally recognised norms in cyberspace and hold violators accountable – a gesture that could also facilitate regional cybersecurity cooperation.

Secondly, South Asian states should organise cybersecurity awareness campaigns to better communicate risks and concerns pertaining to cybersecurity and promote best practices in cyber hygiene. These could include information on the nature of cyber threats facing South Asian societies as well as effective mitigation strategies and incident response measures. These campaigns would facilitate increased participation of the general public in cybersecurity in line with the principle of inclusivity and broad participation of stakeholders that good SSG demands, aligning with UN General Assembly Resolution 58/199 on ‘Creation of a global culture of cybersecurity and the protection of critical information infrastructures’.[16] They would also help foster an interest in the cybersecurity field that could contribute to the development of local cybersecurity talent and expertise, when combined with support for educational and training programmes.

Finally, regional initiatives should be launched in order to exchange best practices and lessons learned in different South Asian states regarding good SSG in cybersecurity. While this would ideally include inter-governmental cooperation, ongoing inter-state tensions make this less likely. In the meantime, exchanges could be established between think tanks, civil society organisations and other non-governmental bodies in South Asia that work on issues pertaining to SSG in cyberspace. Specific areas of cooperation could involve comparing progress on implementing the 11 UN norms and sharing best practices in the development of NCSs.

[16] United Nations (2004) “Creation of a global culture of cybersecurity and the protection of critical information infrastructures”, UN Doc. A/RES/58/199, 30 January, digitallibrary.un.org/record/509571/files/A_RES_58_199-EN.pdf.

Bibliography

Basuroy, T. (2022) “Internet penetration rate in India from 2007 to 2021”, *Statista*, 9 June, www.statista.com/statistics/792074/india-internet-penetration-rate/.

DCAF – Geneva Centre for Security Sector Governance (2021) “Guide to Good Governance in Cybersecurity”, 19 January, www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_EN_Jan2022.pdf.

Hathaway, M. and F. Spidalieri (2021) “Integrating Cyber Capacity into the Development Agenda”, *Global Forum on Cyber Expertise*, thegfce.org/wp-content/uploads/2021/11/Integrating-Cybersecurity-into-Digital-Development_compressed.pdf.

Hogeveen, B. (2022) “The UN norms of responsible state behaviour in cyberspace. Guidance on implementation for Member States of ASEAN”, *Australian Strategic Policy Institute*, www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace.

Insikt Group (2021) “China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions”, *Recorded Future*, 28 February, www.recordedfuture.com/redecho-targeting-indian-power-sector.

International Telecommunication Union (2021) “Global Cybersecurity Index (GCI) 2020”, www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

International Telecommunication Union (2021) “Guide to Developing a National Cybersecurity Strategy – 2nd Edition”, www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf.

Sanger, D.E. and E. Schmall (2021) “China Appears to Warn India: Push too Hard and the Lights Could Go Out”, *The New York Times*, 28 February, www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html.

United Nations (2004) “Creation of a global culture of cybersecurity and the protection of critical information infrastructures”, UN Doc. A/RES/58/199, 30 January, digitallibrary.un.org/record/509571/files/A_RES_58_199-EN.pdf.

Yadav, K., I. Thange, J. Ilhardt, S. Siwakoti and J.N. Shapiro (2020) “Old hatreds fuel online misinformation about COVID-19 in South Asia”, Bulletin of the Atomic Scientists, 25 November, thebulletin.org/2020/11/old-hatreds-fuel-online-misinformation-about-covid-19-in-south-asia/.

Zetter, K. (2016) “That Insane, $81M Bangladesh Bank Heist? Here’s What We Know”, *Wired*, 17 May, www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/.

ASIA-PACIFIC

SECURITY SECTOR
GOVERNANCE NETWORK

Geneva Centre
for Security Sector
Governance

**DCAF – Geneva Centre for
Security Sector Governance**
Chemin Eugène-Rigot 2E
P.O. Box 1360
CH-1211 Geneva 1