রেজিস্টার্ড নং ডি এ-১

বাংলাদেশ গেজেট

অতিরিক্ত সংখ্যা

কর্তৃপক্ষ কর্তৃক প্রকাশিত

মঙ্গলবার, মার্চ ১১, ২০১৪

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার

ডাক, টেলিযোগাযোগ ও তথ্যপ্রযুক্তি মন্ত্রণালয়

তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ

(আইসিটি-১ শাখা)

প্রজ্ঞাপন

তারিখ, ০৩ মার্চ ২০১৪ খ্রিঃ

নং ৫৬.০০.০০০০.০২৮.২২.০০৬.১৪-৩৪—সরকার সাইবার ঝুঁকি নিরসনে "সাইবার সিকিউরিটি স্ট্রাটেজি" অনুমোদন করেছে। ইহা সর্বসাধারণের জ্ঞাতার্থে প্রকাশ করা হলো।

রাষ্ট্রপতির আদেশক্রমে

আর. এইচ. এম. আলাওল কবির
সহকারী সচিব।

মূল্য ঃ টাকা ১৬.০০

NATIONAL
CYBERSECURITY STRATEGY

EXECUTIVE SUMMARY

Bangladesh requires reliable physical and information communication technologies (ICTs). The two types of infrastructure jointly support essential services in sectors such as communications, emergency services, energy, finance, food, government, health, transport and water. Therefore, to achieve our economic security and democratic objectives, we require reliable physical and digital infrastructure. Physical assets increasingly depend upon the reliable functioning of the digital infrastructure or critical information infrastructure (CII) to deliver services and to conduct business. Consequently, significant disruption to CII could have an immediate and debilitating impact that reaches far beyond the ICT sector and affects the ability of a nation to perform its essential missions in multiple sectors. Therefore, critical information infrastructure protection (CIIP) is everyone's responsibility.

This document is *"The National Cybersecurity Strategy of Bangladesh".* It is one of the long-term measures for protecting our cyber world against security threats, risks and challenges to national security. The Strategy addresses the country's national security strategy. The purpose of this document is to create a coherent vision for 2021 keeping Bangladesh secure and prosperous by coordinating government, private sector, citizens and international cyberspace defense efforts.

This *National Cybersecurity Strategy* outlines a framework for organizing and prioritizing efforts to manage risks to our cyberspace or critical information infrastructure. To achieve the aforesaid goals above, this Strategy significantly raises the profile of cybersecurity within our governments and defines clear roles and responsibilities. Cognizant of the shared nature of cyber vulnerabilities, this Strategy also requires a public-private partnership to fix the potential vulnerability of private sector-owned critical infrastructures in banking, utilities and telecommunications sectors against cyber attacks.

In addition, we recognize that cybersecurity is a global challenge that demands truly international solutions. Therefore, we commit ourselves to joining regional and international partnerships creating solutions for addressing the cybersecurity challenge regardless of threat. We, therefore, present this *Strategy* in terms of the Pillars of the International Telecommunication Union's Global Cybersecurity Agenda (GCA). The GCA contains five strategic pillars and seven goals for building collaboration between relevant parties in the fight against cyber threats. We aim to help the GCA become the key framework for creating a secure and safe information society.

STRATEGIC CONTEXT

Bangladesh needs to build confidence and security in the use of ICTs because of the growing sophistication, frequency and gravity of cyber threats. Cyber threats are a concern because the disruption or destruction of critical information infrastructure could potentially have severe economic, social and national security impacts.

Our cyberspace faces a range of threats. Cyber threats range from espionage directed towards obtaining political intelligence to phishing to facilitate credit card fraud. In addition to Government information, espionage now targets the intellectual property of commercial enterprises in areas such as communication technologies, optics, electronics and genetics. The design of the Internet infrastructure facilitates some of the cyber threats due to its borderless, anonymous and cross-border nature. Yet, the same insecure Internet serves as a basis for critical government and private sector services in Bangladesh.

We attach great value to the protection of all types of cyber threats. Indeed, cyberspace is swiftly becoming critical to the control of cyber threat devices linked to the energy and transportation sectors such as electronic transformers and pipeline pumps. New smart grid technologies deliver intelligent monitoring, control, communication and self-healing technologies. However, smart meters are susceptible to unauthorized modification, distributed denial of service and disruption during patching. We are also concerned about an increasing number of cyber attacks. For example, a growing number of cyber attacks aim to steal official government documents detailing negotiating positions. Disclosure of such details would seriously harm our national security and interests.

Worryingly, cyber espionage and other cybercrimes are very low cost activities. Attack tools and methodologies for activities such as phishing or malware distribution are freely available on the Internet even to amateurs. Besides, perpetrators face little risk of conviction due to incompatible legal frameworks and the lack of organizational structures to aid international cooperation, dialogue and coordination in dealing with cyber threats. Silent surveillance enables hostile nations to map the structure and defenses around key government and private sector infrastructures, plant backdoors, create and test attacks.

GOAL

Working collaboratively home and abroad, to manage all major cyber risks that affect us directly irrespective of their origin and type, thereby creating a safe, secure and resilient critical national information infrastructure for our economy and society.

PURPOSE OF STRATEGY

This Strategy recognizes the impact of cyber threats, risks and challenges to our national values and interests. The Strategy underlines the need for concerted effort to counter these fast evolving threats. This fully integrated approach leverages the resources of the Government, organizations across all sectors, individual private citizens and international partners in mitigating threats to our cyberspace. The Strategy defines the organizational structures required to address this embryonic risk to our prosperity and national security.

WAYS – PRIORITIES

The Strategy is the basis for a coordinated national and globally compatible approach to protecting our critical infrastructure against cyber threats. In line with the Global Cyber security Agenda (GCA) of ITU, our strategic Areas are:

- The development of a comprehensive set of national cybercrime legislation that is regionally and globally applicable and harmonized

- The implementation of measures to reduce vulnerabilities in software products through the deployment of accreditation schemes, protocols and standards;
- The definition of strategies for capacity building mechanisms to raise awareness, transfer know-how and boost cyber security on the national policy agenda; and
- The development of a unified national multi-stakeholder strategy for international cooperation, dialogue and coordination in dealing with cyber threats.

Cyber Security Priorities

National Cyber security Strategy should have three national priorities:

- Legal Measures;
- Technical and Procedural Measures; and
- Organizational Structures

The first priority focuses on strategies for the development of cybercrime legislation that is harmonized and applicable globally. The second priority deals with organizational structures and policies on cybercrime, watch, warning and incident response as well as the creation of a generic and universal digital identity system. Priority three focuses on a national framework of security protocols, standards and software accreditation schemes.

Priority 1: Legal Measures

This Priority deals with the enactment of laws to deter and prosecute cybercrime. Inevitably, the actions will depend on national conditions and local needs. The establishment and modernization of laws, procedures, and policy to prevent, deter, respond to, and prosecute cybercrime is an integral component of the *National Cybersecurity Strategy of Bangladesh*. Since cybersecurity is a global challenge, the lack of harmonized national and regional cybercrime legislation weakens Bangladesh's internal and worldwide ability to detect, prosecute and deter cybercrime. The *National Cybersecurity Strategy* identifies the actions below as necessary for creating suitable cybercrime legal measures:

Action 1: Cybercrime Legislation

This Action involves creation of laws that are interoperable and applicable globally.

Our cybercrime legislation shall be harmonized with global conventions. Therefore, we shall align our cybercrime legislation with the ITU Toolkit for Cybercrime Legislation. The alignment of our cybercrime legislation with the ITU Toolkit for Cybercrime helps international cooperation and addresses jurisdictional and evidentiary issues.

Additionally, internationally harmonized legislation strengthens cybersecurity, as it helps our country build capacity for preventing, deterring and prosecuting cybercrime.

The cybercrime law should be evaluated by all ministries and legislative committees that might have an interest in it, even if they have nothing to do with criminal justice, so that no useful idea is missed.

The cybercrime law should similarly be evaluated by the local private sector, by any local affiliate of the international private sector, by local non-governmental organizations, by academics, by unaffiliated interested citizens, by willing foreign governments, and anyone else with a recognized interest.

It is recommended that the text of National Cybercrime law be drafted to comply with the provisions of the Convention on Cybercrime (2001)

Action 2: Government Legal Authority

This Action aims to ensure that governments have sufficient legal authority to secure cyberspace in public interest.

- To create cybersecurity organization structures including the National Cybersecurity Council;
- Defines the legal basis for creating a national CIRT, For example, the Act defines the powers to shutdown a critical infrastructure if at risk of a cyber attack;

- Provides the basis for promoting cybersecurity skills, training and awareness;
- Defines the legal and operational basis for an integrated and fully coordinated public private sector partnership on cybersecurity;
- Fosters innovation in cybersecurity to help develop long-term solutions; and
- Grants the government authority to participate in international cooperation, dialogue and coordination activities focuses on cybersecurity such as mutual assistance.

Priority 2: Technical and Procedural Measures

This Priority addresses the need to create organizational structures at national and regional levels to facilitate communication, information exchange and the recognition of digital credentials across jurisdictions. The structures would help create a generic and universal digital identity system and the necessary organizational structures to recognize digital credentials across jurisdictions through the following actions:-

Action 1: National Cybersecurity Framework

This Action aims to create a Framework that defines mandatory security standards and offers guidance on issues such as risk management, compliance and assurance.

The Bangladesh National Security Framework outlines minimum-security measures that stakeholders must abide by to claim compliance with national cybersecurity requirements. The Framework contains core security values and minimum standards that apply to a wide range of stakeholders. Stakeholders select the applicable standards based on their risk profile and information protection needs. The stakeholders may use an internal audit or external auditor to demonstrate compliance with the minimum-security standards to a central organization. However, the Framework does not provide detailed technical instructions on specific ICT systems.

The *National Cybersecurity Strategy* identifies the following Policy Goals as vital components of the National Cybersecurity Framework:

- Governance and Risk Management

- Information Security and Assurance
- Protective Marking and Asset Management
- Staff Vetting and Clearance
- Physical and Environmental Security

Action 2: Secure Government Infrastructure

This Action deals with spreading awareness of relevant risks, preventive measures and effective responses to government Departments and Agencies.

The Government of Bangladesh owns and operates only a minority of critical information infrastructure. However, Bangladesh attributes considerable importance to the protection of critical information infrastructure. Therefore, the Government will lead the cyberspace security. For example, the Government's procurement process will mandate the inclusion of security clauses in service contracts to encourage development of secure cyberspace technologies. The *National Cybersecurity Strategy* identifies the following actions as vital for securing cyberspace:

- Create and enforce a staff vetting and clearance scheme;
- Create and enforce a formal information or data classification for sensitive data;
- Create and enforce a cybersecurity risk management process across government ministries and agencies;
- Define and enforce a robust government Authentication Framework;
- Improve security in government outsourcing and procurement through vetting of suppliers, incorporation and enforcement of security clauses in contracts;
- Create a vulnerability management process for all government cyber systems;
- Secure government local area networks;

Action 3: Critical Information Infrastructure Protection

This Action focuses on defining a process for tracking and fixing vulnerabilities; improving attack attribution and prevention capabilities.

Vulnerabilities are weaknesses that allow a threat or attack to break a system's confidentiality, integrity and availability defenses. Most of cyber attacks result from poor technical designs or the exploitation of known but unfixed vulnerabilities. The impact of the exploitation of vulnerability depends on the value and criticality of information. Critical information infrastructures inevitably store valuable information.

The *National Cybersecurity Strategy* identifies the following major actions and initiatives to reduce threats and related vulnerabilities in Bangladesh:

- Create a process for national vulnerability assessments to help understand the potential consequences of threats and vulnerabilities;
- Designate important systems as critical information infrastructure and enforce an accreditation regime around them. For example, no system will connect to critical infrastructure without a penetration test and other assurance activities;
- Enhance law enforcement capabilities in the investigation, prevention and prosecution of cybercrimes;
- Require the use of evaluated software products;
- Prioritize national cybersecurity research and development activities;
- Assess and secure emerging systems; and
- Participate in international efforts to improve the security of Internet protocols and routing technologies.

Priority 3: Organisational Structures

This Priority Area requires the building of organizational structures and strategies to help prevent, detect and respond to attacks against critical infrastructure. The *National Cybersecurity Strategy* identifies the actions below as essential for creating appropriate national and regional organizational structures and policies on cybercrime:

Action 1: Government's Cybersecurity Role

Cybersecurity is everyone's responsibility because countermeasures only work well if all relevant stakeholders play their part. The stakeholders include government, business, infrastructure owners and users. Collaboration is vital because neither government nor the private sector can independently control and protect information infrastructure.

The Government of Bangladesh has overall responsibility for securing the infrastructure in public interest. To improve cybersecurity in Bangladesh, it is vital that the Government puts in place appropriate national structures to protect its own infrastructure and all assets required to deliver essential services to the public. The national, regional and globally compatible organizational structures aim to protect classified data and networks against cyber attacks. The Government is also responsible for communicating national priorities to the private sector to help ensure that critical infrastructure under private sector in areas such as banking, transport and telecommunications receives sufficient protection.

To address the cybersecurity challenge, the Government of Bangladesh may appoint a senior aide as the National Cybersecurity Coordinator.

The official has the responsibility to establish a cross-government programme to address the priority areas of this Strategy. The official provides strategic leadership and ensures the coherence of cybersecurity activities across government. The role cuts across government agencies and the official reports to the National Cybersecurity Council, as and when formed. The Coordinator has direct access to the Head of Government as well as sufficient staff and financial resources to coordinate inter-gvernment activities at a strategic level.

Action 2: National Cybersecurity Council

The National Cybersecurity Council is the focal point for coordinating efforts to protect our cyberspace. This multi-Council body unites operational cybersecurity

efforts of government institutions and leads collaboration with industry. Public-private partnership coordination is critical to protecting our critical infrastructure because it enhances information sharing and cooperation on cyber threat identification, incident response and recovery. The *Cybersecurity Strategy* mandates the Council to perform the roles below:

- Developing a comprehensive national plan for securing critical infrastructure and services whether in government or private sector;
- Providing national major incident response capacity in an event of significant attacks on critical infrastructure;
- Providing government and private sector organizations strategic advice and processes for managing cybersecurity Programmes;
- Providing integrated security advice (combining information, personnel and physical) to the government agencies and businesses owning or operating critical information infrastructure to reduce its vulnerability to cyber and other threats;
- Acting as the National Technical Authority for Information Assurance for private sector organizations and government agencies in all aspects of cybersecurity;
- Working with other government agencies including intelligence agencies to review threat and vulnerability information and distribute advice on the countermeasures to regional and local governmental organizations, private sector, academia and the general public;
- Engage in international schemes such as the International Multilateral Partnership Against Cyber Threats (IMPACT) for alerts, early warning and cooperation;
- Perform and fund research and development with other agencies to create a new generation of secure cyber technologies. An annual review assesses the effectiveness of the Council's cybersecurity activities.

Action 3: National Incident Management Capacity

Timely identification, communication and recovery from major cybersecurity events and weaknesses affecting critical information infrastructure can often mitigate the damage resulting from malicious cyberspace activity. Best practice indicates that these efforts are most effective at national level because they provide wider participation in analysis, warning, information gathering, vulnerability reduction, mitigation and recovery. Inevitably, the government needs to work with the private sector to coordinate a national response because private firms own the infrastructure and often have better skills. The government creates legal and regulatory incentives to encourage critical infrastructure owners and operators to ensure that their systems are resilient to attacks. This Strategy identifies the following actions regarding cyber incident response:

- Build Bangladesh Computer Incident Response Team (BD-CIRT) at the National Cybersecurity Council;
- Establish a public-private framework for responding to major cyber incidents;
- Encourage development of business continuity and disaster recovery capacity;
- Develop strategic and tactical cyber attack and vulnerability assessment capacity;
- Encourage the development of private sector capacity to share status information about the health of cyberspace;
- Coordinate processes for voluntary participation in the development of national public-private continuity and contingency plans;
- Create a Cyber Warning and Information Network at Cybersecurity Council; and

- Develop mechanism to share information about cyber attacks, threats and vulnerabilities with the public and non-governmental bodies locally and globally;
- Where possible, it is advisable for units to have at least basic computer forensic capacity. Such capacity will require software tools and additional training.

Action 4: Public-Private Partnerships

The commercial sector owns and operates most of the critical infrastructure that Bangladesh relies on home and abroad. Clearly, the Government alone cannot secure cyberspace since it does not own or operate the infrastructure. Therefore, the Government of Bangladesh should form meaningful partnership with the private sector on cybersecurity. The *National Cybersecurity Strategy* requires the Government of Bangladesh and its agents to consult the private sector in the development, implementation and maintenance of regulation, cybersecurity initiatives and policies. Cooperative relationships with the private sector are vital because they:

- Facilitate the exchange of information on the development of new legislation and regulation between stakeholders;
- Enable collaborative work and sharing of training courses that could help alleviate the severe shortage of skilled cyber security professionals; and
- Enable real time exchange of information about cyber threats and vulnerabilities

The communication channel is valuable for the BD-CIRT as the exchange complements the stretched national incident detection and warning resources.

With private sector input, the Government shall also develop a coordinated national strategy for participating in major international discussions that shape policy in areas such as territorial jurisdiction, sovereign responsibility and the use of cyberspace for war. Additionally, the Cybersecurity Coordinator or an equally empowered party works with government departments and agencies, the private sector and academia to formulate and coordinate Bangladesh's international cybersecurity positions. Thereafter, the ministries of Foreign Affairs should work on improving international cooperation.

Action 5: Cyber security Skills and Training

The Action focuses on the creation of programmes to increase the capability of cybersecurity professionals in Managerial, Technical and Information Assurance areas.

This Action requires the initiation of a programme to train a cadre of citizens to secure information flows. This Action focuses on the training of professionals, not creating general awareness. This *Cybersecurity Strategy* identifies the following major activities:

- Adopt a national Cybersecurity Skills Framework;
- Create a continuum of cybersecurity job descriptions;
- Identify commercially available cybersecurity certifications;
- Deliver or manage commercial delivery of training or certification examinations;
- Periodically measure Cybersecurity skills and training levels;
- Invest in mainstream cybersecurity education and research;
- Build cybersecurity capacity of national companies; and
- Work with global partners such as IMPACT to coordinate cybersecurity training;

It is important that prosecutors and judges have some understanding of areas such as computers, software, and networks as well as of the increasing importance of electronic evidence. Similarly, legislators should have some understanding of those topics and of whether a country's laws are adequate to address cybercrime. It may also be helpful to train senior policy-makers, government officials, about the threats to electronic networks (for example, how the national banking system could be attacked) and about the threats posed by electronic networks (for example, the use of the Internet to locate vulnerable children for sexual trafficking).

Action 6: National Culture of Cybersecurity

The Action focuses on the need to raise awareness about cyber threats and the role all relevant stakeholders must play to secure their part of cyberspace. Many cyber threats materialize due to insecure user activities. The users could be end users or system administrators. A lack of awareness coupled with a general lack of skilled cybersecurity professionals increases the likelihood that attackers would trick users into performing insecure activities. On the contrary, user awareness helps create a cybersecurity culture that in turn reduces the likelihood and impact of cyber attacks. This Cybersecurity Strategy identifies the following major activities:

- Promotion of a national awareness programme to empower end users – at home or general workforce – to secure their own cyberspace-linked systems;
- Implementation of a cybersecurity awareness programme for government systems that contain classified data;
- Encouraging cybersecurity culture development in business enterprises;
- Adding cybersecurity awareness to the national education curriculum as a way of spreading knowledge to pupils and their relatives;
- Engaging civil society in outreach to children and individual users;
- Promotion of private-sector support for professional cybersecurity certifications;

Nations are increasingly dependent on complex systems and information technology. In many cases, information and communications technologies (ICT) vital to national and economic security are subject to disruption from a number of causes, either originating from within or outside the nation. Leaders in government and private industry are increasingly confronted with uncertainty about cyber risk and vulnerabilities. This uncertainty stems from the complexity and interconnectivity of evolving technology used to support critical systems. To ensure security and economic vitality, nations must manage cyber security in accordance with their own economic, social, and political considerations.

মোঃ নজরুল ইসলাম (উপসচিব), উপপরিচালক, বাংলাদেশ সরকারি মুদ্রণালয়, তেজগাঁও, ঢাকা কর্তৃক মুদ্রিত।
শাহ্-ই-আলম পাটোয়ারী, ভারপ্রাপ্ত উপপরিচালক, বাংলাদেশ ফরম ও প্রকাশনা অফিস,
তেজগাঁও, ঢাকা কর্তৃক প্রকাশিত। web site: www.bgpress.gov.bd