International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 6, Issue 2, ISSN No. 2455-2143, Pages 213-230
Published Online June 2021 in IJEAST (http://www.ijeast.com)

A COMPREHENSIVE CYBERSECURITY FRAMEWORK FOR AFGHANISTAN'S CYBERSPACE

Ahmad Nabi Ahmadi
Dept. of Electronics and Communication Engineering,
Maulana Azad National Institute of Technology, Bhopal
Madhya Pradesh, India

Abstract: **Need for cyber security framework to protect the evolving ICT Infrastructure and Cyberspace in the modern information society does not need any emphasis. Given the importance of cyber space for country development, many countries have invested large amount of money for cyber space application. Since, based on official documents, Afghanistan is in the process of integrating ICT into its critical information infrastructure, to this end, the country may face various challenges including cyber security. Due to various potential threats and risks to Afghanistan cyber security, a comprehensive cyber security infrastructure and strategy is necessary. Accordingly, Afghanistan has introduced an ICT security law. However, nowadays internet is involving great portion of government and non-government sections. The country must introduce a comprehensive and appropriate cybersecurity framework and strategy to tackle all of the issues and risks related to this arena. With the introduction of different ICT based technologies in the country, Afghanistan is moving towards embracing electronic culture in its day-to-day dealings. As these technologies are becoming popular and being widely used, it is important to put in place technological infrastructure and legal frameworks, which will safeguard the private and enterprise data flowing through these ICT based infrastructures. The aim of this paper is to propose a comprehensive cybersecurity framework for Afghanistan's cyberspace in order to protect and assure data, information and IT infrastructure security in cyberspace, enhance capacities to prevent and response to cyber threats, protect the nation from the risk and vulnerability, damage from modern cyber threats and incidents through a variety of standardized institutional structures, policies and procedures, and eventually establish and achieve a Safe – Secure and Resilient cyber space for the government, businesses and citizens of Afghanistan.**

Keywords: **Cybersecurity, Cyberspace, ICT Infrastructure, Cybersecurity Infrastructure, Cybersecurity Framework, Critical Information Infrastructure, Cyber-attacks**

I. BACKGROUND:

Cybersecurity framework is an evolving task that caters to the whole spectrum of ICT users and providers such as home users, large enterprises, and government as well as non-government entities. It's an umbrella framework for outlining and leading those things connected with the security of cyberspace. Cybersecurity framework allows the individual sectors and organizations to design appropriate cybersecurity strategies to satisfy their requirements in dealing with cyberspace challenges. The framework offers a breakdown of what is needed to effectively protect critical national information infrastructure, information systems, and companies as well as an insight into the government's approach for the protection of cyberspace in the nation. In addition, the collaboration between public and private sectors are fundamental players to protect the country's critical national information infrastructure. Therefore, the strategy aims to construct a cybersecurity framework, leading to certain actions with programs to improve the cybersecurity and cyberspace of the nation [1]. Offered the importance of critical national information infrastructure for the nation's development, different countries have cataloged and analyzed their relevant critical information infrastructure. ICT sector or cyberspace depends on Critical Information Infrastructure (CII) which can be accessed via the internet or elsewhere, as well as goes beyond territorial boundaries, this will make protecting this infrastructure more complex. It is for this reason why international cooperation and collaboration plays a central part in the national cyber security strategy (NCS), whenever infrastructures are interconnected, new vulnerabilities might arise from the common links, failures might propagate through the varied systems, intrusion, and disruption in one infrastructure might provoke unanticipated threats to others. In such conditions, the question of specifying dependability and trust requirements and translating them as performance and functionality requirements for other systems becomes vital. At the local and international level, cooperation and coordination amongst countries appear crucial to have a comprehensive approach. An extensive framework for cybersecurity and critical information infrastructure security would involve a national strategy and the creation of legal frameworks to curb cyber-crime [2].

1) Threats to Cybersecurity Infrastructure:

Today internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies are changing, but due to these emerging technologies, we have not been able to protect our private information in an exceedingly effective way because cyber-attacks are increasing every day. Nowadays more than sixty percent of total commercial transactions are done online, and this field requires a top quality of security for transparent and best transactions. Hence cybersecurity is becoming a big issue. The scope of cybersecurity isn't just limited to securing the information in the IT industry but additionally to various other fields [3]. A cyber-attack can be an attack that is mounted against us (meaning our digital devices) through cyberspace. Cyber threats can be an enormous deal, cyber-attacks can originate electric blackouts, failure of military equipment, and breaches of national safety secrets [4].

Types of Cybersecurity Threats:

1) Malware: Software that performs a malicious task on a target network, e.g. corrupting data or taking up a system.
2) Phishing: An email-borne attack that involves tricking the e-mail recipient into disclosing tips or downloading spyware by clicking on a hyperlink inside the message.
3) Spear Phishing: A more sophisticated kind of phishing where the attacker learns in regards to the victim and impersonates somebody he/she knows and trusts.
4) Man in the Middle (MitM) attack: Where an attacker creates a side between your sender and recipient of electronic messages and intercepts them, possibly changing them in transportation. The sender and recipient believe they're communicating directly with each other.
5) Trojans: Named after the computer virus of ancient Greek language history, the Trojan may be a sort of spyware that enters a target system looking like something, e.g. a typical software application, on the other hand, lets out of the malicious code once inside the host system.
6) Ransomware attack: An attack that involves encrypting information on the prospective system and demanding a ransom in return for permitting the user to have access to your information once again. These attacks consist of serious incidents just like the locking down of the complete town of Atlanta's neighborhood government data.
7) Distributed Denial of service Attack (DDoS): Where an attacker gains many (maybe thousands) of devices and utilizes them to invoke the functions of a target system, e.g. overwhelm a target website with fake traffic.
8) Attacks on IoT Devices: IoT devices like commercial sensors are susceptible to multiple sorts of cyber threats. Included in these are attack and unauthorized access to data being collected by the product Given their numbers, geographic distribution and regularly out-of-date operating systems, IoT devices are a definite major target for malicious actors.
9) Data Breaches: a data breach can be a theft of real information by a malicious actor.
10) Malware on Smartphone Apps: Cellphone devices are vulnerable to malware attacks a bit like other computing equipment. Cyber-criminals may embed malware in application downloads, mobile websites, or Phishing emails and text messages. Once compromised, a smartphone will give the attacker access to

non-public information, location data, financial accounts and more [5].

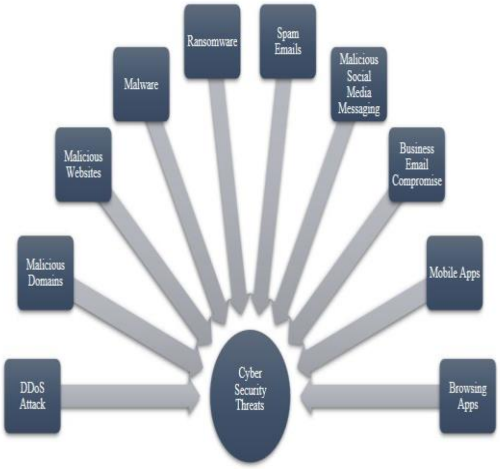
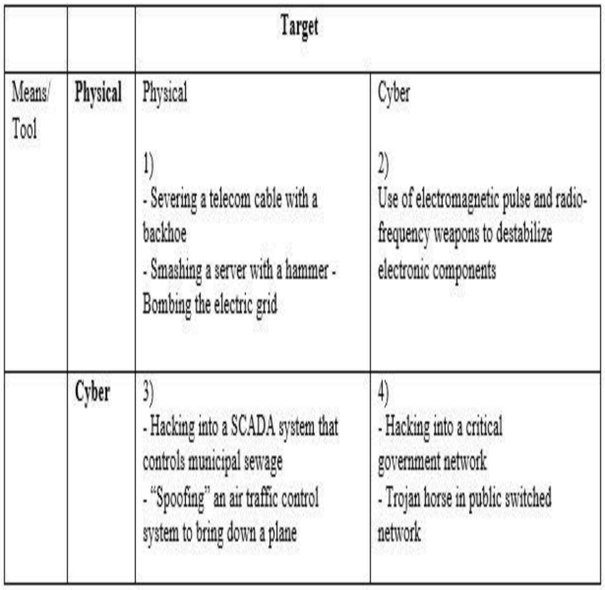


Fig.1. Threats to Cybersecurity

2) Threats to ICT Infrastructure:

Means to hack, disrupt, and destroy data resources consist of hacker tools to products like electromagnetic weapons; directed energy weapons; HPM (High Energy Microwave), or HERF (High Energy Radio Frequency) guns; and electromagnetic pulse (EMP). The attack against an information infrastructure is usually administered with both physical implements (hammer, bomb, HERF, HPM) and cyber-based hacking tools. An equivalent is true for the goal: It is usually cyber, consisting for example of information or applications for a network, or physical, like computer systems or even a telecommunications cable. The infrastructure threat matrix (Table 1) distinguishes four kinds of information attack, all four of which involve the malicious utilization of the understanding of the infrastructure, either being a target or as being a tool [6].



		Target	
Means/ Tool	Physical	Physical 1) - Severing a telecom cable with a backhoe - Smashing a server with a hammer - Bombing the electric grid	Cyber 2) Use of electromagnetic pulse and radio-frequency weapons to destabilize electronic components
	Cyber	3) - Hacking into a SCADA system that controls municipal sewage - "Spoofing" an air traffic control system to bring down a plane	4) - Hacking into a critical government network - Trojan horse in public switched network

Table.1.Infrastructure Threat Matrix

II. AFGHANISTAN'S CHALLENGE:

Afghanistan as a developing Middle East country which in terms of cybersecurity is at its rudimentary stage, needs a comprehensive cybersecurity infrastructure to survive in such a competitive world. Correspondingly, MCIT Afghanistan quotes:

"With the introduction of various ICT based technologies within the country, Afghanistan is moving towards embracing electronic culture in its day-to-day dealings. As these technologies are getting popular and being widely used, it's important to place in situ technological infrastructure and legal frameworks, which can safeguard the private and enterprise data flowing through these ICT based infrastructures. MCIT has already drafted an ICT law which has addressed broader cybersecurity-related issues but so as to completely implement the Law there's need for further development of regulations in additional focused areas".

It also emphasizes that data privacy will support: Entrepreneurs for e-commerce; the government to run e-administration and e-services and therefore the public so as to share their personal data with the government also as enterprises through e-service delivery channels. Correspondingly, consistent with

The International Telecommunication Union (ITU) reports [7], Afghanistan has three challenging issues regarding cybersecurity. First, there's no appropriate mechanism in order to detect, identify, and deter cyber threats and risks within government sectors. Second, some agency computers aren't equipped with suitable and reliable protection software, that is, antivirus, for blocking malware and viruses. Third, officials performing in governmental and non-governmental sectors and organizations have little or no knowledge about cybersecurity and cyber-attacks and the way they will be targeted, and the way they will identify and stop such incidents. Furthermore, some government agencies state that they have never experienced any cyber-attack, this will be associated with two possible issues, either they're not wanting to share the knowledge regarding the attack, or they're unaware of the attacks. Additionally, the country's cyber network is far dispersed and spread, and the detection of cyber-attacks incidents in such environment is extremely complicated and difficult. Additionally, no agency appears to possess any related information concerning cybersecurity policies or procedures which are in place. Also, no Government agencies are fully having any knowledge about numerous cybersecurity standards available which will be adopted to surge security, including COBIT, FISMA, ISO/IEC 27001, and ITIL. Afghanistan needs a comprehensive cybersecurity framework and infrastructure in order to tackle the cyberspace security issues. Since Afghanistan is within the process of integrating ICT into its critical information infrastructure, the country may face various challenges regarding cyberspace, a comprehensive cybersecurity infrastructure and strategy are required for Afghanistan. Since the internet has penetrated both the government and non-government sectors with various cyber applications. Thus, the country must introduce a comprehensive and appropriate cybersecurity infrastructure and strategy to tackle all the problems and risks associated with this arena. The aim of this research is to propose a cybersecurity strategy framework for Afghanistan to guard the country's critical national information infrastructure within the process of integrating ICT and cyber services in providing social and economic services. Therefore, to the present end, after a radical and comprehensive literature survey, research, and evaluation of the cybersecurity frameworks and strategy of over eight developed countries, a comprehensive cybersecurity framework is developed, which covers every aspect of Afghanistan's cyberspace. There are some key challenges faced by the ICT sector in Afghanistan that has got to be addressed in order to achieve the secure cybersecurity framework and strategy goals [8]:

1) Cybersecurity isn't allocated sufficient priority in politics and on the continued ICT projects. Also, Cybersecurity principles aren't adopted by the governmental and non-governmental organizations.

2) Critical National Information Infrastructure (CNII) has not been recognized and there's no defined cybersecurity strategy in place to manage and mitigate cybersecurity incidents just in case if an organized cyber-attack is done on the critical national information infrastructure. It had been recommended that the Country should develop a National Cyber Security Strategy which will clearly define the roles of the varied stakeholders and develop measures and procedures for the protection of CNII.

3) Appropriate legislation, policies, and regulations on cybersecurity are inadequate to deal with the present cybersecurity challenges.

4) Training, specifically within the area of cybersecurity must be improved; all stakeholders like Regulators, Enforcement Agencies, Judiciary, Prosecutors, Service providers, Financial Institutions, Service providers got to have adequate capacity and capability to handle matters associated with cybersecurity.

5) There is no proper coordination or mechanism handling monitoring, detection, tracking, and mitigation of cyber-attacks and cyber threats at the national level. There's no coordination on cybersecurity issues, it had been

6) Recommended that the country should establish a National Computer Emergency Response Team to watch and detect cyber threats, also as educate the general public.

7) The country should develop and implement awareness campaigns to teach about cyber laws, the impact of cybercrime, and measures of combating it [9].

III. LITERATURE REVIEW

An extremely less amount of research contributions towards nationwide cybersecurity framework had been made formerly. However, the comprehensive research that this paper is focused on is considered to be able to fulfill an investigation gap. To state the ideas behind developing cybersecurity framework and strategy three individuals Azmi, Tibben and Win adapted a literature review of the National Cyber protection Strategy in a worldwide context. The review [10] used a qualitative comparison approach amongst (54) countries and consequently the findings reveal key reasons behind creating a cybersecurity strategy. It suggests the need for making a cybersecurity strategy. The main downside was, the conclusions they reached were based on the study of current National Cybersecurity Strategy (NCSS) themes. Which means the dependability of the concepts could not be guaranteed. Another situation study performed by the National Cyber Bureau of Israel on the Cybersecurity policy model proposed a framework for the creation of cybersecurity Framework. The case study [11] was relative research between the National Cybersecurity Strategy (NCSS) of nations that are considered world pioneers in technology. The analysis had been conducted by Deniel Benoliel. The study discovered some most readily useful applications that have been followed by all of the nations tangled up in the cross-comparison. However the limitation of this study is every country has some distinct agenda, therefore they certainly will have some differences while creating their techniques due to distinct nationwide and international interests. The framework is workable that can be considered as a confident aspect. Comparable works in the area of cybersecurity methods have been adopted by different authors. However, insignificant attempts had been made formerly to evaluate the Cybersecurity Infrastructure and Framework of Afghanistan in the comparison to other countries. Therefore this research will make up for the research gap found in this context. Since the national cybersecurity infrastructure of Afghanistan is concerned, the strategy outlines a framework for organizing and prioritizing efforts to handle risks of Afghanistan's cyberspace which directly accompanies the GCA (Global Cyber Security Agenda). In line with the GCA, this infrastructure implies the prioritization associated with the strategic areas.

IV. METHODOLOGY:

1) Research Type:

This research requires gathering relevant information from the specified documents related to the intended topic. Therefore, qualitative research will be followed in this study in order to analyze and ultimately propose a comprehensive Cybersecurity framework and strategy for Afghanistan's cyberspace.

2) Method to Carry Out Research:

The research method that will be used is analyzing other country's cybersecurity framework and strategy in a cross-comparison with the cybersecurity framework of Afghanistan's cyberspace that will help to understand the strength of the cybersecurity policy of Afghanistan's cyberspace. A brief review for the cybersecurity strategy of Afghanistan will be done with respect to the cross-comparison between other countries national cyber security strategy (NCSS). Eight other countries have been chosen as the comparison vector. Cybersecurity strategies of the (USA, UK, Israel, Japan, South Korea, Malaysia, Singapore, and India) will be studied and analyzed. Those analyzed data will be categorized into some criteria that are already been suggested as standards for a cyber-security strategy framework by the Israeli National Bureau of Cybersecurity. That categorized information will then be compared side by side with the cybersecurity Infrastructure of Afghanistan. Thus, this study also employs a qualitative approach using the semi-structured interview to propose a comprehensive cybersecurity Infrastructure based on the cybersecurity experiences of the developed and developing countries. As an outcome of conducting a comprehensive literature review, cyber threats, cybersecurity, and global cybersecurity strategy are discussed. In addition, Afghanistan's ICT status as well as Cybersecurity are identified. The developed and developing countries' experience in cybersecurity has also been underlined. To recognize the status of ICT and cybersecurity in Afghanistan, the people in charge were interviewed. Then, the threats to Afghanistan's cyberspace are underlined. The Afghanistan cybersecurity Infrastructure is then

Analyzed (but the country has only general ICT law). Finally, a cybersecurity framework is proposed for Afghanistan. The framework consists of ten Strategies in order to secure the ICT infrastructure in country and eventually establish and achieve a Safe –

Secure and Resilient cyberspace for the government, businesses, and citizens of Afghanistan. Thus, the current research proposes the following main strategy pillars with their corresponding objectives illustrated as follow:

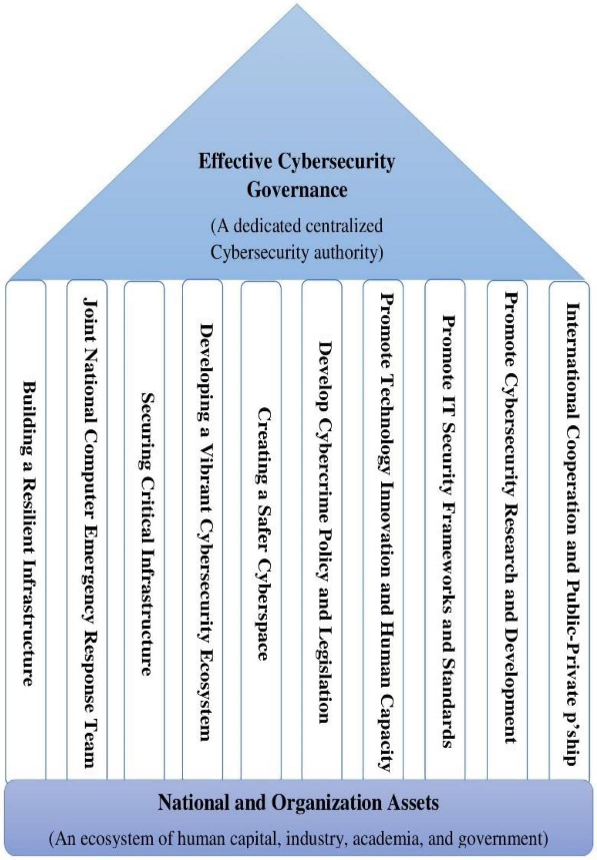

Effective Cybersecurity Governance
(A dedicated centralized Cybersecurity authority)
Building a Resilient Infrastructure
Joint National Computer Emergency Response Team
Securing Critical Infrastructure
Developing a Vibrant Cybersecurity Ecosystem
Creating a Safer Cyberspace
Develop Cybercrime Policy and Legislation
Promote Technology Innovation and Human Capacity
Promote IT Security Frameworks and Standards
Promote Cybersecurity Research and Development
International Cooperation and Public-Private p'ship
National and Organization Assets
(An ecosystem of human capital, industry, academia, and government)

Fig.2. a Comprehensive Cybersecurity Framework for Afghanistan's Cyberspace

Effective Cybersecurity Governance

The essential & most important factor of the proposed framework is an effective cybersecurity governance which in the organizational aspect is an effective strategy and action plan and without it, it is impossible to handle and implement this comprehensive framework. Two constructs of cybersecurity are significant to this study: governance and management. The phrase governance is accustomed to express a system for controlling or managing, which includes the process of controllers and regulators. Whereas the term Management is adopted to refer to the communication of the responsibilities of controllers and regulators, by using executive actions [12]. Governance consists of the clarity of requirements for decision-making, setting rules, responsibilities, and the boundaries for the autonomy and actions of the involved parties. The part of governance is not handling, but defining the extent of management. Considering cybersecurity, the governance focuses on what the businesses need to do differently or increase what's accepted nearly as good information safety governance practices [13].

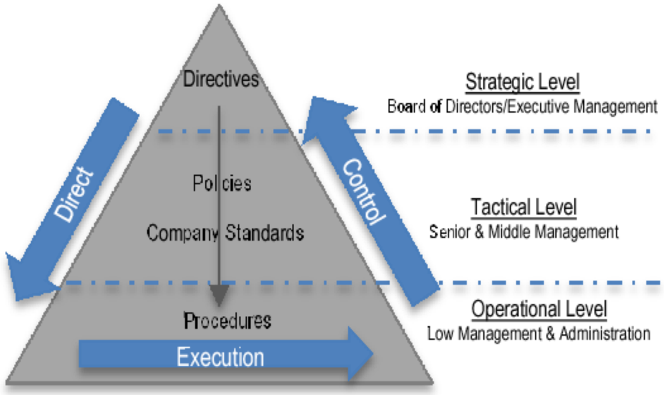


Fig.3. Effective Cybersecurity Governance

1) Cybersecurity Governance:

Cybersecurity governance is the management system by which a business directs and controls cybersecurity. The governance framework determines who is authorized to make decisions and how accountability will be founded for outcomes. IT Governance spans the culture, organization, policy, and methods that provide for IT management and control across five key functions including Strategic Alignment, Value Delivery, Resource Management, Performance Management, and Danger Management. Governance processes provide oversight to secure that risks are adequately mitigated.

Cybersecurity governance program focused to initiate and keep a framework to offer assurance that information security strategies are aligned with, and support business goals are constant with applicable regulations through constancy to policies and interior settings. The objectives of an organization may vary with the sort of business organization type, although the following are the major goal of governance program [14]:

- Protect the infrastructure of the business and its stakeholders by keeping a cyber-safe environment.
- Controlling security policies that address each aspect of safety strategy, controls, and regulation.
- Secure a complete set of criteria for each policy to guarantee that procedures and guidelines comply with the policy
- Secure risk management processes are funded, maintained, and monitored for proper technology's risk management.
- Control the IT implementation & operations of the company and protect its critical assets.
- The success or collapse of the company protection program is properly checked by establishing metrics and monitoring processes to make sure compliance, provide feedback on the effectiveness and give you the basis for appropriate management decisions.
- Control the action of users and ensure that technology resources are used responsibly (educational and other policies that may apply to the employment of technology resources, data handling, etc.)
- Secure compliance requirements are met for the concerned organization [15].

2) Cybersecurity Organizational Structure:

An Organizational structure of data safety or cybersecurity is a structured management framework that directs, monitors, and controls the execution & procedure of cybersecurity in the Organization. The cybersecurity organizational structure is the dwelling created by organization leadership and includes formal organizational charts, documented policies, and directives. In all government organizations, Chief Information Security Officer (CISO) should be provided with an appropriate level of government support, resources, and funding to manage the cybersecurity implementation and operation. This structure clearly defines functions and responsibilities for cybersecurity inside a company after various sort of reporting models considering criticality and sensitivity for the information being handled by the organization [16].

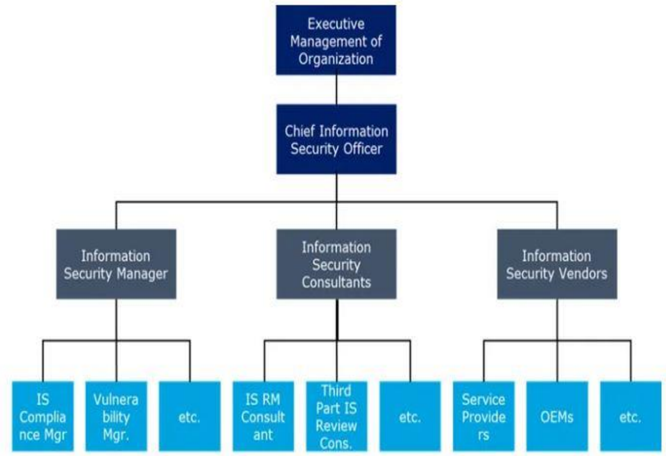

Executive Management of Organization
Chief Information Security Officer
Information Security Manager
Information Security Consultants
Information Security Vendors
IS Complia nce Mgr
Vulnera bility Mgr.
etc.
IS RM Consult ant
Third Part IS Review Cons.
etc.
Service Provide rs
OEMs
etc.

Fig.4.Cybersecurity Organizational Structure

Building a Resilient Infrastructure

Behind the scenes, in every government, a scope of essential services and infrastructure are needed to keep a modern metropolis running smoothly. Essential services such as energy, banking, healthcare, and transport are powered by ICT. Cyber-attacks on these Critical Information Infrastructures (CIIs) can restrain these essential services. At best, they lead to inconveniences. At worst, they will end in significant disruptions to the economy and to our society. Afghanistan government has got to make sure that its critical information infrastructures (CIIs) aren't just resilient against physical threats, but also against cyber threats. A cyber-resilient infrastructure will provide safer cyberspace to Afghanistan's citizens, a cyber-resilient infrastructure will reinforce confidence in Afghanistan as a resilient and trusted global center of trade and commerce. The government should concur with main stakeholders and the CII operators because of the cybersecurity framework - in four major areas:

- Strengthen the protection of our essential services.
- Intensify our capability to respond comprehensively to cyber-attacks.
- Strengthen our cybersecurity governance and legislative Framework.
- Make Government systems more secure.

To firm our digitally-enabled economy and to make our country more resilient against cyber-attacks, the Government should work with key stakeholders, Private sector operators and the cybersecurity community to strengthen the resilience of our Critical Information Infrastructure (CII). And for this reason the government must intensify the CII Protection program to regulate robust and systematic cyber risk management processes across all critical sectors. The government must upgrade these sectors' response and recovery plans against cybersecurity breaches. The government must set up multi-sector cybersecurity exercises to test cooperation across multiple sectors and address inter-dependencies during major cyber-attacks. Ultimately, as threats to government networks will continue to grow, we will expand efforts to secure government systems and networks [17].

Joint National Computer Emergency Response Team

A Computer Emergency Response Team (CERT) is just a group of data safety experts responsible for the protection, detection, and response to an organization's cybersecurity incidents. A CERT may focus on resolving incidents like data breaches and cyber-attacks additionally providing alerts and incident handling guidelines. CERTs additionally conduct ongoing public awareness campaigns while having interaction in research geared toward increasing protection systems. In line with the proposed cybersecurity Infrastructure and framework, the government needs to establish a joint national computer emergency response group made up of private, public, and military sectors to develop cooperative ties. A few of the main and key Functionalities associated with the national computer emergency response group are as follow [18]:

- Setting up a 3-tier defense system connecting international gateway, ISPs, and end-users (organizations and customers) in purchase to detect and block cyber-attacks in advance.
- Strengthening response systems in the economic sector by reinforcing security systems in banking institutions and expanding safety monitoring services to insurance firms and credit card corporations.
- Reinforcing cyber restoration system by developing and distributing anti-virus pc software for the exclusive use of Zombie PCs to simply help rapid recovery and boosting cooperative relations between the private as well as the public sectors.
- Gathering, analyzing, and dissemination of information on cyber incidents.
- Forecast and alerts of cybersecurity incidents.
- Emergency measures for managing cybersecurity incidents.
- Coordination of cyber incident response activities.
- Subject guidelines, consolatory, vulnerability records, and whitepapers relating to Cybersecurity practices, procedures, prevention, response, and reporting of cyber incidents.

Securing Critical Infrastructure

In today's highly interconnected world, Cyber-Physical Systems (CPS) link computerized control systems and real devices that communicate using their environment to supply a wide variety of services that people depend on every day. In general, Critical Information Infrastructure (CII) is those information and technology infrastructures upon which the core functionality of Critical Infrastructure depends. A Critical Infrastructure (CI) is made up of a group of systems and assets, whether physical or virtual, so necessary to the state that any disruption of their services could have an urgent impact on national protection, economic well-being, and general public health. These Critical Sectors are (Energy, Transportation, Law enforcement agencies, Banking and Finance, Telecommunications, Defense, Space, Public Health, Water Supply, Critical manufacturing, E-governance, Power generation, Nuclear Industry). A few of the main characteristics of Critical Infrastructures are high Complexity, Interconnection, Interdependence, and Distribution. Despite the increased specialization in securing OT environments, critical organizations are nevertheless attempting to find a far better approach when it involves industrial cybersecurity. Fortunately, there certainly are a handful of actions that each organization can use to reduce risk across their critical infrastructure [19].

Secure the central components of industrial operations:

Programmable Logic Controllers (PLCs) are central points towards the operation of Operational Technology (OT) surroundings. These products command the pumps and motors and robots that power massive utility and manufacturing plants. Regular programming modifications to the PLC could additionally be normal, but they will also be a consequence of a software mistake or malware that affected an unauthorized modification. Self-activating of configuration changes maintains a “last known good state” of your control systems and preserves an audit trail of any changes being made. Recording this activity, at particular intervals or any moment users create a change, is a significant effort in decreasing danger around your most crucial infrastructure assets.

Gain full visibility across OT Infrastructure:

Organizations that separately deploy IT and OT protection leave critical blind spots in their wake. Attacks are designed to infect and propagate throughout the converged IT/OT infrastructure. While most organizations have some visibility into their IT footprint, additionally it is essential to use a full stock of OT assets in your environment. Far from IT devices which frequently have a lifespan of 36 months, OT devices can keep a lifespan of years. Over that time, teams often change, upkeep may become lax as well as in most cases, and meticulous documentation of things like patches and firmware updates are missed. By deploying industrial-grade protection that may view your complete organization’s infrastructure, alongside asset inventory right down to ladder logic and backplane information.

Use various detection methodologies to identify threats early:

Gaining deep situational awareness of every asset in the (CII) environment is crucial for protecting common infiltration points and targets of cyber-attacks. It is equally important to stay observant in what passes over your system, keeping in mind that network traffic and behavior are very early caution indications for attacks and attack propagation [20]. Decreasing attack risk requires multi-detection capabilities which include policy, anomaly, and signature-based detection. Using numerous detection methods can prevent both known and zero-day attacks, while also leveraging the facility of the security community to seek out more threats and therefore secure the environment from more assaults earlier.

Focus reformative efforts on critical assets and actual exploits:

Whatever OT vendors are present in your infrastructure, chances are you’ll see many vulnerabilities announced over their product lifetimes. In fact, critical infrastructure organizations often operate with many thousands of vulnerabilities at any given time! It is often unmanageable and impractical to trace and remedy all of these vulnerabilities with new ones being announced a day. The good news is you don’t have to. Risk is primarily related to vulnerabilities that become exploits. Once you've got an in depth understanding of the precise vendors, model numbers, patch levels, and firmware versions inside your OT environment, you'll utilize functionality that identifies the vulnerabilities and exploits most relevant to your environment. With a prioritized list of vulnerabilities, supported asset criticality, and sort of exploit, you’ll be ready to triage your response and reduce the highest-risk elements first to stay your environment secure [21].

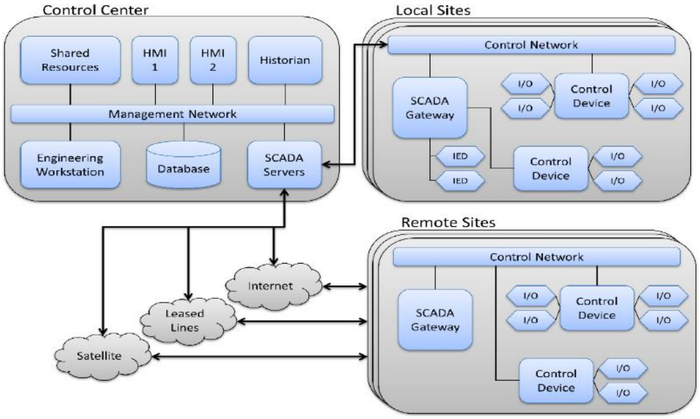


Fig.5. Architecture of a Generic SCADA Network

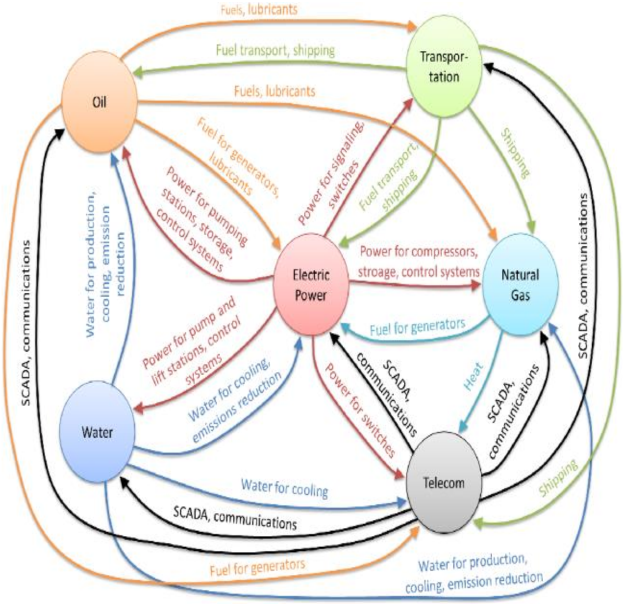

Fuels, lubricants
Fuel transport, shipping
Fuels, lubricants
Transpor-tation
Oil
Fuel for generators, lubricants
Power for pumping stations, storage, control systems
Power for signaling switches
Fuel transport, shipping
Shipping
Electric Power
Power for compressors, stroage, control systems
Natural Gas
Fuel for generators
Water for production, cooling, emission reduction
SCADA, communications
SCADA, communications
Power for pump and lift stations, control systems
Water for cooling, emissions reduction
SCADA, communications
Power for switches
Heat
SCADA, communications
Water
Telecom
Water for cooling
SCADA, communications
Shipping
Fuel for generators
Water for production, cooling, emission reduction

Fig.6. Critical Infrastructure Interdependencies

Developing a Vibrant Cybersecurity Ecosystem

The cybersecurity ecosystem carries a wide range of contributors, private firms, non-profits, governments, individuals, processes, and cyber devices (computers, software, and communication technologies) that interact for multiple purposes. To evolve highly skilled professionals, companies with deep cybersecurity capabilities, and strong translational research and development (R&D) the government of Afghanistan should establish and promote a vibrant cybersecurity ecosystem. The ecosystem will ensure a sustainable source of experience and solutions to support our plans for resilient national infrastructure and safer cyberspace. It will also bring economic opportunities to the residents and Afghanistan-based companies. Afghanistan's cybersecurity industry is dynamic and fast-growing. Furthermore, integrating cybersecurity service offerings with industry sectors in Afghanistan will enhance our competitive advantages in these areas. The Government must work with industry partners, professional associations, and research institutes in three main areas [22]:

Establish a professional workforce:

The government must encourage existing cybersecurity professionals to develop their careers in the industry by determining clearer pathways, promoting internationally recognized certifications, and building strong communities of training. To grow the workforce, we'll attract promising students through scholarship and sponsorship programs. We will additionally help new entrants to the profession with an industry-oriented curriculum for students as well as up-skilling and re-skilling opportunities for mid-career specialists.

Innovate to accelerate the industry's growth:

The government must establish and start the national cybersecurity Research and Development (R&D) Program to support research into both technological and human-science aspects of cybersecurity. We will sustain this effort with world-class R&D facilities and focused talent development programs. In order to achieve this goal the government has to promote R&D collaborations between the government, academia, and industry to engender faster and more market-relevant R&D outcomes.

Creating a Safer Cyberspace

Digital integration has both empowered and endangered businesses and individuals. It opens new social and commercial opportunities, yet also exposes citizens to criminal syndicates across the planet. By using computing devices, these cybercriminals can steal data, extort money, and attack networks, causing harm to others. Cyberspace must be kept safe and trustworthy for businesses and individuals. Cyber technology can enable and empower business and society, but as long as it's safe and trustworthy. Securing cyberspace is the collective responsibility of the government, businesses, and individuals. To secure cyberspace, the government must establish and initiate the National Cybercrime Action Plan (NCAP), furthermore, the government should work with international institutions, other governments, industry partners, and Internet Service Providers (ISPs) to quickly identify and reduce malicious traffic on our Internet infrastructure. Ultimately, Enterprises and business associations can play their part by fostering their members' understanding of cybersecurity issues and promoting the adoption of excellent practices [23]. In order to make Afghanistan's Cyberspace safer and more secure the government must work on following key areas:

Fight cybercrime through the National Cybercrime Action Plan (NCAP):

First and foremost the federal government must establish and lunch a National Cybercrime Action Plan (NCAP) to ascertain a coordinated national effort to impact cybercrime. Then the government should educate and enable the basic public to remain safe in cyberspace because it is easier to stop a cybercrime from occurring within the first destination. 2nd, Furthermore, The government must strengthen legislation and the criminal justice framework. This will assist in the investigation of cybercrimes and prosecution of cybercriminals. Ultimately, the government must intensify partnerships and international engagement to manage the rapidly evolving nature of cybercrime and tackle cross-border issues.

The action of each business and individual make a difference to our collective safety in cyberspace. Companies and individuals must keep informed and take preventive measures to secure their computer systems and digital devices, particularly to stop malicious actors from hijacking their systems and devices to cause harm to other people. Organizations and business associations usually take the lead to make cybersecurity a concern and touch on government cybersecurity expertise to improve their members' understanding of cybersecurity issues and encourage the adoption of good practices [24].

Develop Cybercrime Policy and Legislation

The Internet has allowed cybercriminals to commit cybercrimes quickly, effortlessly, and on a large scale. Cybercriminals have exploited the anonymity provided by the web and the transnational nature of cybercrime to bypass detection and prosecution. These characteristics of cybercrime pose significant challenges for legislation enforcement agencies around the globe [25]. As the use of the Internet becomes more predominant in Afghanistan, the number of cybercrime cases has increased sharply. Acknowledging the need for a concerted and coordinated national effort to effectively handle cybercrime, the Ministry of Communications and Information Technology jointly with the Ministry of Home Affairs (MHA) must lunch the National Cybercrime Action Plan (NCAP). The NCAP will set out the Government's key principles and priorities in combating cybercrime. The Plan will also detail the Government's ongoing efforts and plans to tackle cybercrime. The vision of the NCAP is to ensure a safe and protected online environment for Afghanistan. The NCAP has three priority areas:

1) Up-skilling and empowering the public to stay safe in cyberspace:

Prevention is the best way to combat cybercrime; the bulk of cybercrime are often prevented if businesses and individuals are educated on the risks of cybercrime and adopt simple cybercrime prevention measures to protect themselves online. In order to coach and empower the overall public to stay safe in cyberspace. The government of Afghanistan must establish the Afghan Cyber Police (ACP) command, which will be the complete community of cyber police responsible for regularly sharing cybercrime prevention messages with the overall public via various media platforms, such as television, newspapers, social media, text messages, and posters at conveyance nodes and lifts publicly housing blocks. Alongside with its Public Cyber-Outreach & Resilience Program, ACP must use behavioral insights to aware the general public to adopt good cyber hygiene practices. ACP will also adjust its cybercrime prevention outreach programs to match the profile of various vulnerable groups in society, thereby ensuring that the message of cybercrime prevention is effectively communicated to all segments of society. By way of its Collaborative Social Program, ACP will work with schools, universities, institutes and non-governmental Organizations (NGOs) to share cybercrime prevention awareness among vulnerable groups. The ACP must also create an online self-help portal against scams and frauds. The portal will provide information to the general public on the various types of scams and frauds for empowering the general public to require steps in order to protect against them [26].

2) Improving the Government's capacity and capability to combat cybercrime:

The international nature of cybercrime, like the speed and scale at which such crimes are conducted, presents formidable challenges for traditional enforcement approaches. For an effective battle against cybercrime, the government must: 1. establish the ACP cybercrime prevention command, 2. boost cybercrime research capabilities, 3. equip public officers with the appropriate skills to combat cybercrime, and 4. improve coordination between ACP and government [26].

3) Industry and Academia Partnership:

Deep expertise to influence cybercrimes need not simply reside with the federal government and may also be located within the private sector and academia. Given the rapidly evolving nature of cybercrime [27]. The government has to improve awareness of cybercrimes in the private sector. And the government must regularly engage key private sector stakeholders to enhance cybercrime prevention efforts, raise awareness of cybercrimes, and encourage the adoption of good cyber hygiene practices, the government must also collaborate with the private sector to jointly develop capabilities to answer the latest cyber threats.

For instance, the ACP has to partner with local research institutes to develop new cybercrime investigations and forensics capabilities.

Promote Technology Innovation and Building Human Capacity

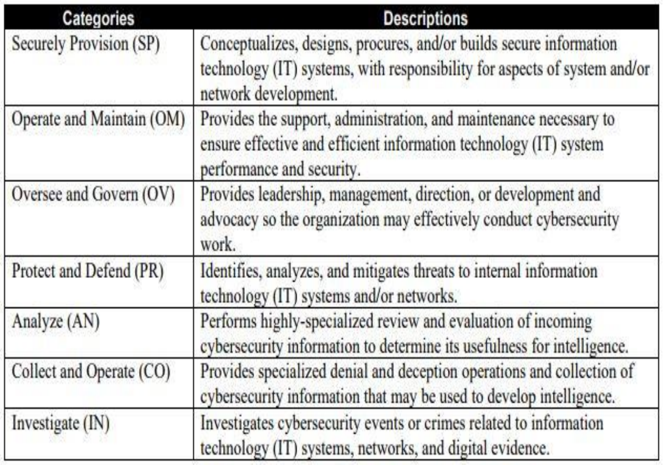
1) Technology Innovation for Cybersecurity:

Due to the powerful nature of cyber threats and attacks, governments are required to simply take appropriate measures to get along aided by the latest technologies useful for detecting and addressing cyber threats. To remain updated with the latest findings in this field, research is mandatory [28]. Hence, it's recommended that Afghanistan must adopt Technology innovation to explore new cybersecurity initiatives also to remain safe and more secure against cybersecurity threats. The increased complexity of this communication and networking infrastructure is making the prevention of cybercrimes difficult that is increasing the demand for cutting-edge technologies and new approaches to secure cybersecurity infrastructure. Some of those cutting-edge technologies are:

- Artificial Intelligence
- Block-Chain
- Quantum Computing
- 5G Mobile Technology
- Internet of Things (IoT)
- Modern Cryptography
- Big Data
- IT-OT Convergence

2) Building skilled Human Capacity for Cybersecurity:

To evolve a more resilient and skillful cybernation, we must have a highly-skilled cybersecurity workforce across Industries and government. Effective cybersecurity workforce development helps organizations to efficiently recruit qualified cybersecurity professionals, and to provide this critical workforce with clear job descriptions and development opportunities. The cyber domain is a multi-disciplinary joining of computer science, mathematics, economics, law, psychology, and engineering. It encompasses not only the networking of online devices together, but how humans interact and are influenced by these devices. As such, the cyber domain impacts every domain of modern life from the electricity that powers millions of homes to the transportation network that moves millions of people daily. As the number and uses for connected devices grow, the complexity of cyber infrastructure grows exponentially, as do the number of vulnerable devices. The cybersecurity workforce supports this infrastructure and defends our networks [29]. The Department of Homeland Security's National Initiative for Cybersecurity Careers and Studies (NICCS) developed a Cybersecurity Workforce Framework to provide a base set of work roles for the cyber workforce. Although this ontology was developed to support US government hiring requirements and was not empirically justified, it represents the well-documented listing of work roles in the cyber domain. This collection includes nine work-role categories, 31specialty areas, and over 1000 types of knowledge, skills, and abilities. Major categories are described in Table 2. Considering Afghanistan's case study regarding skilled cybersecurity workforce: There is a huge gap in existing cybersecurity professionals from Afghanistan government. So in order to fill this gap which is more important for creating a safer cyberspace in Afghanistan, the government should establish and initiate their own cybersecurity workforce framework, which will represent a well-defined list of work roles in Afghanistan's cyber domain.



Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Table.2. US-Cybersecurity Workforce Framework

Promote IT Security Frameworks and Standards

The challenges of running a cybersecurity governance and management program at national level are often overwhelming with numerous areas to deal with, from encryption to application security to disaster recovery. The issue of compliance with regulatory requirements like HIPAA and PCI DSS. An IT security framework may be a series of documented processes to define policies and procedures around the implementation and ongoing management of data security controls in an enterprise environment. These frameworks are generally a blueprint for building an information security program to manage risk and reduce vulnerabilities. Frameworks are often customized to unravel specific information security problems, a bit like building blueprints are customized to satisfy their required specifications and use. Some frameworks were developed for specific industries, also as different regulatory compliance goals, they also are available with varying degrees of complexity and scale. There is a huge amount of overlap in these frameworks in terms of general security concepts as each evolves. Many frameworks provide guidance on where to start when securing your organization from common cybersecurity threats. Most begin with basic practices and processes that are essential to the inspiration of your cyber risk reduction management. With the assistance of the simplest cybersecurity frameworks. These top cybersecurity frameworks will allow your organization to realize a more cyber resilient program. By utilizing these frameworks, many government organizations consider cybersecurity to be a priority. The need to implement effective cybersecurity strategies grow every day. Cybercriminals always derive more sophisticated techniques for executing attacks. This has led to the event of varied frameworks meant to help organizations in achieving robust cybersecurity programs. For that reason, Enterprises understand the highest cybersecurity frameworks for enhancing their security postures [30]. Cybersecurity frameworks ask for defined structures containing processes, practices, and technologies which companies can use to secure network and computer systems from security threats. Some of the main cybersecurity frameworks are as discussed below:

- ISO 27000 series
- COBIT
- NIST Special Publication 800-53
- NIST Special Publication 800-171
- NIST Improving Critical Infrastructure Cybersecurity
- CIS Controls (formerly the SANS Top 20)
- HITRUST CSF

The choice to use a specific IT security framework is often driven by multiple factors. The type of industry or compliance requirements might be deciding factors. Publicly traded companies will probably want to stay with COBIT. The ISO 27000 series is the work of art of data security frameworks with applicability in any industry, although the implementation process is long. NIST SP 800-53 is the standard required by U.S. federal agencies but could even be employed by any company to create a technology-specific information security plan. The HITRUST CSF integrates well with healthcare software or hardware vendors looking to supply validation of the safety for their products. Amongst all these any of it will help a security professional organize and manage an information security program [31].

The only bad choice among these frameworks isn't choosing any of them. Considering Afghanistan Cyberspace regarding Information Security Frameworks, unfortunately there is no proper knowledge and understanding of common cybersecurity standards or regulatory frameworks in Afghanistan’s government and non-government organizations, in order to overcome this problem the government of Afghanistan must promote the implementation and understanding of these Frameworks in government and private organizations**.**

Promote Cybersecurity Research and Developing

There is a huge demand for investment in cybersecurity capacity building, Research and Development (R&D) activities. To define a cybersecurity research and development roadmap for the country all the stakeholders, government, industry, and academia have to come together. To develop a securer cyber ecosystem Public-Private Partnership (PPP) would help in combining the best of both worlds and complement capabilities. Talent in this field has to be retained in the country. Proper security measures to the property rights (IPRs) developed by the indigenous cybersecurity research organizations have got to be arranged. Increased government-funded research and public-private coordination are needed in the expanding fields of new secure networking and computing architectures, high-performance computing, encryption, data integrity, artificial intelligence, big data, privacy, and risk management strategies. Governments have to provide legal protections for legitimate and beneficial computing privacy and security research. Governments around the world are involved in continuous research within the field of cybersecurity to safeguard against emerging and future threats. It is always good to find out from others and not waste resources in reinventing the wheels. Some of the cybersecurity research areas that are focused by US government are briefly mentioned [32]. U.S. Government Federal Cybersecurity Research and Development Strategic Plan Implementation Roadmap, has identified the following six areas critical for successful cybersecurity Research and Development:

- Scientific foundations.
- Enhancements in risk management.
- Human aspects.
- Transitioning successful research into pervasive use.
- Skilled workforce development.
- Enhancing the infrastructure for research.

A set of guiding principles are formulated to ensure the cybersecurity program addresses the desired improvements, outcomes, and guidance stated in the policy document. The following are guiding principles specific to the cybersecurity domain [33]:

1) Organize research activities to systematically progress towards achieving the attributes and desired end state of a healthy cyber ecosystem.
2) Social science research labs to understand social science dimensions of cybersecurity, augmenting "hard computer science" research.
3) Research on comprehensive scientific approaches that comprehensively and rigorously underpin required security policy.
4) Research on promising scientific approaches that comprehensively and rigorously underpin the quantitative cybersecurity risk assessment of complex systems especially critical infrastructure.• research on promising scientific approaches to robotize joint function amongst distributed systems to defend individual computers and networks.
5) Research that recognizes the presence of adversaries in cyberspace, with potential emphasis on the Manichean sciences.
6) Occupy research labs to investigate cybersecurity-related research gaps and to determine scientific approaches and emerging technological solutions.
7) Depend on present knowledge that is relevant to cybersecurity.
8) Strengthen research that addresses big data challenges that also addresses cyber challenges.

International Cooperation and Public-Private Partnership

The cyber environment is not limited to the physical boundaries of the countries. Successful cybersecurity initiatives require international cooperation. Best practice, intelligence, discussing challenges, and learning from others' mistakes as well as assisting in formulating and driving international strategy direction along with initiative would help Afghanistan secure the critical national information infrastructures [34]. Cyber threats don't respect sovereign boundaries and cyber-attacks can emanate from almost anywhere within the world. Malicious actors have deliberately exploited jurisdictional gaps between countries to their advantage. Moreover, with countries increasingly connected to at least one other through trade, global logistics, and financial markets, cyber-attacks disrupting one country can have serious spillover effects on other countries. Developing partnerships between government authorities and infrastructure owners and operators may be a method to assist the stability and availability of critical information and communication technologies. Partnership amongst government and industry helps the government disseminate vital information about security threats and vulnerabilities, coordinate effective incident management, and understand the resilience of critical infrastructure. The same partnership can help industry become aware of information about threats and vulnerabilities to which it would not normally have access and improve the industry's ability to manage risk, As an international member, we have supported and contributed to regional efforts to build cybersecurity capabilities. Through consensus, agreement, and cooperation, cyberspace is often a safer place for all, to achieve this, Afghanistan's government will:

Forge national and international cooperation to counter cyber threats and cybercrime:

We will continue working closely with the international community and international partners to strengthen platforms and procedures for cyber incident reporting and response. We will work with international Member States to coordinate the regional approach to cybercrime. We will also strengthen resources to tap the worldwide operational networks and capabilities to tackle cybercrime [35].

Facilitate exchanges on cyber norms and legislation:

We will continue to participate in international and regional discussions on cyber norms, cyber policy and legislation, cyber deterrence, and cybercrime cooperation. We will host an annual Afghanistan International Cyber Week (AICW) to catalyze, stimulate, and promote exchanges on cybersecurity and cybercrime issues.

V. RESULTS AND DISCUSSIONS:

Based on the experiences of some developing and developed countries (USA, UK, Israel, Japan, South Korea, Malaysia, Singapore, and India), in terms of cyber protection strategy, and also predicated on the findings of both document content analysis and interview, it's found that Afghanistan has a drastic development in terms of ICT services in the social and financial aspects over the past decade. However, it was found that even though the country experienced cybersecurity issues, there is no cybersecurity infrastructure and framework in place. Therefore, Afghanistan, as an ICT appearing country, which is increasingly providing ICT-based solutions, requires a comprehensive cybersecurity strategy infrastructure and framework to deal with the challenges of cyber threats. Correspondingly, the Ministry of Communications and Information Technology, Afghanistan must give priority to guard the federal government data and investment. Consequently, in this research, the primary focus associated with the proposed comprehensive cybersecurity infrastructure framework is to protect government information, critical information infrastructure, and safe cyberspace.

Recommendations:

The research gave recommendations as follows:

1) To strengthening security systems, the government should open a dedicated cybercrime center. Meanwhile, the government has to continue to seek new opportunities for international co-operation.
2) Information security agencies have to work with policymakers to take a broad view and to treat attacks on computers and infrastructure the same way. The government should not separate the protection of infrastructure from the applications that run on top of it.

3) The government should collaborate with telecom sector, banking, transport, and public sectors to adopt risk management measures and to report significant incidents to competent authorities.

4) Cybercrime conducted in one application, could provide access to other applications the user uses. Therefore it is borderless in nature and makes cybercrime investigations more complicated for law enforcement authorities. To effectively tackle cybercrime, adequate cross–border provisions are needed, and international cooperation and mutual assistance within the region law enforcement needs to be enhanced.

5) The government must understand that the Cybersecurity framework is a living document that helps an organization define their current and desired cybersecurity state, identify areas of need, and how well they are progressing in that direction, as well as advice On how to communicate to internal and external stakeholders about risks that threaten services.

6) Cybersecurity is a global issue, it is no longer just a single business or single country issue. Therefore, it requires cooperation from governments and industry alike to recognize cybersecurity as a shared global problem. Hence, the government must encourage all stakeholders consider doing the following:

- Revise security policy documents to adopt and reflect the language and vocabulary of the framework.
- Establish regular procedures for identifying new threats, testing security procedures, and updating procedures to address those threats, thereby establishing an adaptive cybersecurity program.
- Ensure that senior management is active in establishing a cybersecurity strategy for the company and reviewing the implementation of that strategy.

VI. CONCLUSION

In the proposed research work, the present status of Afghanistan’s Cybersecurity and ICT infrastructures in Afghanistan were investigated and the threats to Afghanistan's cyberspace had been highlighted. The Afghanistan cybersecurity strategy ended up being also examined and had been found that Afghanistan has no cybersecurity strategy framework in a destination. This had generated proposing a comprehensive cybersecurity strategy infrastructure and framework for Afghanistan’s cyberspace. Cyberspace, cyber threats, critical information infrastructure, cybersecurity strategy framework, and global cybersecurity strategy, in general, were talked about in line with the literature review just before distinguishing the Afghanistan cybersecurity and ICT status. To determine the status of cybersecurity and ICT in Afghanistan, the crucial findings of research work were analyzed after which the issues and threats to Afghanistan cyberspace were highlighted followed by analyzing the Afghanistan cybersecurity strategy. Finally, an extensive cybersecurity infrastructure and framework with ten pillars were proposed for Afghanistan's cyberspace and ICT context. The findings of the current research could assist Afghanistan develops or modifies the comprehensive cybersecurity strategy based on the experiences of the developed countries. Thus, the government can address the dilemmas of cybersecurity. Although this research has proposed a comprehensive cybersecurity framework for Afghanistan, it's been evaluated through case studies. It is suggested that for future research the proposed cybersecurity framework be tested in the real situation.

VII. REFERENCES

[1]. Walid, al-Ahmad. (2013). A Framework for a Corporation Cyber War Strategy. Paper presented at the 2nd International Conference on Informatics Engineering & Information Science in Malaysia (ICIEIS2013), Nov. 12-14, Kuala Lumpur. Vernez, G. 2013. The Development of the Swiss Cyber Security Strategy. Information Warfare, 17.

[2]. Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructures: attack and defense modeling. Systems, Man and Cybernetics, Part A: Systems and Humans. *IEEE Transactions,* 40(4): 853-865.

[3]. Avanti Kumar. (“July/ Aug 2013. 7. CIO Asia, September 3rd, H1 2013”). IEEE Security and Privacy Magazine – IEEECS “Safety Critical Systems – Next Generation “: Cyber security in Malaysia

[4]. Al Mazari, A.; et al. (2018). Cyber terrorism taxonomies: definition, targets, patterns, risk factors, and mitigation strategies. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, pp. 608–621. IGI Global, Hershey

[5]. G. Magklaras and S. Furnell, (2010). “Insider threat specification as a threat mitigation technique,” in Insider Threats in Cybersecurity, ser. Advances in Information Security, C. W. Probst,J. Hunker, D. Gollmann, and M. Bishop, Eds. Springer US, vol. 49, pp. 219–244

[6]. Chaturvedi, Manmohan & Gupta, MP& Bhattacharya, Jaijit. (2009). Cyber Security Infrastructure in India: A Study. Pp.1-15. https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10 .1.1.542.8083

[7]. ITU. (2012). *Readiness assessment for establishing a national CIRT (Afghanistan, Bangladesh, Bhutan, Maldives, and Nepal*). Telecommunication Development Sector. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/CIRT_Assessment_ABBM N_countries_final.pdf

[8]. Ministry of Communication and IT, E-Government Directorate, E-Government Resource Center. (December 05, 2015) *DRAFT CYBERSECURITY PLAN*. Unknown Place of Publication: Ministry of Communication and IT. [Online] [Accessed on 28th March 2020] https://mcit.gov.af/sites/default/files/2020-08/DRAFT%20CYBER%20SECURITY%20PLAN% 20%20Dec%205%202015_0.pdf

[9]. National Cybersecurity Strategy Republic of Botswana Ministry of Transport and Communications. *National Cybersecurity Strategy*. Unknown Place of Publication: National Cybersecurity Strategy Republic of Botswana Ministry of Transport and Communications. [Online] [Accessed on 25th March 2020] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Rep ository/00042_02_botswana-national-cybersecurity- strategy.pdf

[10]. R. (December 2016). Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy. Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy. Retrieved. https://www.researchgate.net/publication/308470260_ Motives_behind_Cyber_Security_Strategy_Dev

[11]. Towards a Cyber Security Policy Model – Israel National Cyber Bureau (INCB) Case Study. (2015, January 07). Retrieved May 24, 2017. https://publixphere.net/i/noc/page/IG_Case_Study_To wards_a_Cyber_Security_Policy_Model_Israel_Natio nal_Cyber_Bureau_INCB

[12]. Fidler, Bradley. (2017). Cybersecurity Governance: A Prehistory and its Implications. Digital Policy, Regulation and

Governance. 19. 00-00. DOI: 10.1108/DPRG-05-2017-0026.

[13]. Bodeau, D., Graubart, R., and Fabius-Greene, J., Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels, The MITRE Corporation, 2009, PR 09-4656, http://www.mitre.org/work/tech_papers/2010/09_4656 /09_ 4656.pdf

[14]. Asgarkhani, M., Correia, E., & Sarkar, A. (2017). An overview of information security governance. 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET). doi:10.1109/icammaet.2017.8186666

[15]. Asgarkhani, M.: Corporate ICT Governance: A Tool for ICT Best Practice. Proceedings of the International Conference on Management, Leadership, and Governance. 1: 1-8. 978-1-909507-00-5. (2013)

[16]. AlGhamdi, S., Win, A. K. T., & Vlahu-Gjorgievska, D. E. (2020). *Information Security Governance Challenges and Critical Success Factors: Systematic Review. Computers & Security, 102030.* doi:10.1016/j.cose.2020.102030

[17]. TER, K. L. (2018). *Singapore's cybersecurity strategy. Computer Law & Security Review, 34(4), 924–927.* doi:10.1016/j.clsr.2018.05.001

[18]. SPSW Strategy Series: Focus on Defense and International Security. (2014*) Review of the Japan Cybersecurity Strategy:* Issue No. 290. Unknown place of publication: ISPSW Strategy Series: Focus on Defense and International Security. [Online] [Accessed on 5th April 2020] https://www.files.ethz.ch/isn/183668/290_Nitta.pdf

[19]. Taylor, J. M., & Sharif, H. R. (2017). *Security challenges and methods for protecting critical infrastructure cyber-physical systems. 2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT).* doi:10.1109/mownet.2017.8045959

[20]. Butts, J., & Shenoi, S. (Eds.). (2014). *Critical Infrastructure Protection VIII. IFIP Advances in Information and Communication Technology*. DOI: 10.1007/978-3-662-45355-1

[21]. Department of Defense (DOD). (2019). Defense critical infrastructure program. Available athttps://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-Global-Security/Defense-Critical-Infrastructure-Program/Accessed 25 June 2019

[22]. Hsu, F. D., & Marinucci, D. (2013). Advances in Cyber Security: Technology, Operation, and Experiences. Fordham University Press. doi:10.5422/fordham/9780823244560.001.0001

[23]. Goodman, S.E. and Lin, H.S., Editors (2007). "Toward a Safer and More Secure Cyberspace". Washington, D.C.: National Academies Press.

[24]. Cyber Security Agency of Singapore. (2016) *Singapore's Cybersecurity Strategy*. Unknown place of publication: Cyber security Agency of Singapore. [Online] [Accessed on 5th June 2020] https://www.csa.gov.sg/news/publications/singapore- cybersecurity-strategy

[25]. Bressler, Martin & McMahon, R. & Pence, D. & Bressler, Linda. (2015). Fighting Cybercrime Calls for Effective Strategy. Journal of Technology Research.

[26]. World Bank and United Nations. 2017. Combatting Cybercrime: Tools and Capacity Building for Emerging Economies, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

[27]. Rajamaki, J. (2018). Industry-university collaboration on IoT cyber security education: Academic course: "Resilience of Internet of Things and cyber-physical systems." 2018 IEEE Global Engineering Education Conference (EDUCON). doi:10.1109/educon.2018.8363477

[28]. Elkhannoubi, Hasna & Belaissaoui, Mustapha. (2015). Fundamental pillars for an effective cybersecurity strategy. 1-2. 10.1109/AICCSA.2015.7507241.

[29]. Dawson J and Thomson R (2018) the Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. Front. Psychol. 9:744.doi: 10.3389/fpsyg.2018.00744

[30]. Riza Azmi, William Tibben & Khin Than Win (2018): Review of cybersecurity frameworks: context and shared concepts, Journal of Cyber Policy, DOI:10.1080/23738871.2018.1520271

[31]. Nnolim, A.L. (2007), *A Framework and Methodology for Information Security Management*, Lawrence Technological University, Southfield, MI.

[32]. the White House (2011), *Cyberspace Policy Review, Assuring a Trusted and Resilient Information*, www.whitehouse.gov/assets/documents/Cyberspace_P olicy_Review_final.pdf

[33]. T. Benzel, "A Strategic Plan for Cybersecurity Research and Development" in *IEEE Security & Privacy*, vol. 13, no. 04, pp. 3-5, 2015.doi: 10.1109/MSP.2015.84

[34]. Spencer, Fm. (2017). Public-Private Partnerships (PPP) for Cybersecurity Infrastructures. DOI: 10.13140/RG.2.2.22703.59044.

[35]. Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 4362

- Elkhannoubi, Hasna & Belaissaoui, Mustapha. (2015). Fundamental pillars for an effective cybersecurity strategy. 1-2. 10.1109/AICCSA.2015.7507241.

- Azmi, Riza & Tibben, William & Win, Khin. (2016). Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy.

- Min, Kyoung-Sik & Chai, Seung-Woan & Han, Mijeong. (2015). an International Comparative Study on Cyber Security Strategy. International Journal of Security and Its Applications. 9. 13-20. 10.14257/ijsia.2015.9.2.02.

- Hindawi. Journal of Engineering Volume 2020, Article ID 5267564, 19 pages. https://doi.org/10.1155/2020/5267564

- Atoum, Issa & Otoom, Ahmed & Ali, Amer. (2014). A holistic cyber security implementation framework. Information Management & Computer Security. 22. 10.1108/IMCS-02-2013-0014

- Telecommunication Union (ITU), The World Bank, Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organization (CTO), NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE). 2018. *Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity*. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO)