RS Global Journals

Scholarly Publisher
RS Global Sp. z O.O.
ISNI: 0000 0004 8495 2390

Dolna 17, Warsaw, Poland 00-773
Tel: +48 226 0 227 03
Email: editorial_office@rsglobal.pl

JOURNAL	International Journal of Innovative Technologies in Social Science
p-ISSN	2544-9338
e-ISSN	2544-9435
PUBLISHER	RS Global Sp. z O.O., Poland

ARTICLE TITLE	A STUDY ON THE CURRENT "NATIONAL CYBER SECURITY STRUCTURE" IN MONGOLIA
AUTHOR(S)	Sukhbaatar Shirbazar, Baasandamba Dashtseden
ARTICLE INFO	Sukhbaatar Shirbazar, Baasandamba Dashtseden. (2024) A Study on the Current "National Cyber Security Structure" in Mongolia. *International Journal of Innovative Technologies in Social Science*. 2(42). doi: 10.31435/rsglobal_ijitss/30062024/8184
DOI	https://doi.org/10.31435/rsglobal_ijitss/30062024/8184
RECEIVED	12 May 2024
ACCEPTED	25 June 2024
PUBLISHED	27 June 2024
LICENSE	This work is licensed under a **Creative Commons Attribution 4.0 International License.**

A STUDY ON THE CURRENT "NATIONAL CYBER SECURITY STRUCTURE" IN MONGOLIA

Sukhbaatar Shirbazar
Colonel, Mongolia

Baasandamba Dashtseden
Brigadier general, Ph.D, Mongolia

DOI: https://doi.org/10.31435/rsglobal_ijitss/30062024/8184

ARTICLE INFO

Received 12 May 2024
Accepted 25 June 2024
Published 27 June 2024

KEYWORDS

National Security, Cyber Security, Cyber Space, National Cyber Security System.

ABSTRACT

According to one of the six components of Mongolia's national security concept, the country's national cyber security structure was established within the framework of the "On National Security," "On Cyber Security," and "On Armed Forces" laws. Despite these efforts, Mongolia's information and cyber security remain inadequate. Consequently, there is an urgent need to enhance the unified national system for protecting Mongolia's cyberspace.
This involves clearly defining the roles and functions of the state, society, and citizens, as well as updating policies and legal regulations to ensure coordinated efforts among the organizations involved in the system.

Citation: Sukhbaatar Shirbazar, Baasandamba Dashtseden. (2024) A Study on the Current "National Cyber Security Structure" in Mongolia. *International Journal of Innovative Technologies in Social Science*. 2(42). doi: 10.31435/rsglobal_ijitss/30062024/8184

Introduction.

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes. Global cyber security has become increasingly volatile, with countries defining cyberspace as the fifth domain of war and combining cyber operations with other spaces.

Cyberspace is an open international space that encompasses the four domains we have been given naturally: land, water, air, and space. It can be accessed by individuals, states, hostile parties, and terrorists. Missions in Cyberspace The specific level and scope of the need for control of cyberspace is dependent on the specific activity conducted in, though, and from cyberspace. In general, there are six classes of activities.

They are:

✓ constructing cyberspace,
✓ passive defense,
✓ active defense,
✓ exploitation or operational preparation of the environment,
✓ attack,
✓ defining the needed capabilities to conduct defined missions in, though, and from cyberspace.

The fundamental imperative for maturing understanding is to treat cyber as a place, not a mission. That is, cyberspace is a domain in, from, and through which military operations create intended effects.

The fundamental military objectives relative to this domain are essentially the same as in the other domains, again – land, sea, air, and space. The primary objective is freedom of action in, though, and from cyberspace as needed to support mission objectives. The corollary is to deny freedom of action to adversaries at times and places of our choosing. The ability to do both provides for cyber military superiority.

Similarly, air superiority requires control of selected areas at all times and other areas at selected times. The same is true of cyberspace. Even so, there remains significant confusion about the concept of cyber superiority.

Cyberspace governance, in particular cyber rules-making, move from principles to action. After years of arduous bargaining among multiple actors, the macro-structure of global cyberspace governance seems to be on the horizon. Just like global governance in other areas, rules are also at the heart of global cyberspace governance. Cyber rules can be divided into two levels: general rules (abstract principles) and specific rules on a concrete subject matter. The international community, especially the United Nations Group of Governmental Experts on information security, has reached important consensus on such general rules as cyber sovereignty and cyber freedom, and acknowledged that international law, and in particular the Charter of the United Nations, is applicable to cyberspace. In the future, all parties should go beyond general rules and abstract principles and move toward specific and concrete rules that are of pragmatic value. Of course, there are different types of cyber rules dealing with diverse cyber threats, such as cybercrimes, cyber terrorism, cyber warfare, data leakage (privacy protection), and technological vulnerabilities (technical standards).[1]

Current situation of Syber Security in Mongolia.

The problem of protecting the national cyber security has expanded to include not only ensuring the protection, integrity, and accessibility of information in this space but also the protection of national security from cyberattacks and aggression carried out through this space.

A System theory suggests that Mongolia's cyber security is largely influenced by global trends. This means that our cyber safety relies on developments in information technology worldwide, including advances in other countries' cyber defenses and military capabilities. It's also affected by the creation of cyber weapons and harmful software. Therefore, in order to determine the global cyber security environment, I have been studying the national cyber defense structures of various countries.

The governance organization and national cyber defense structure of 62 countries have been studied in detail. According to the results of the research, these countries are providing their own national cyber defense systems. In general, the country's cyber security systems can be classified as follows:

It includes:

✓ Defense sector or Armed Forces-based system.
✓ The system based on the organization of intelligence.
✓ Independent Cyber Security Agency Framework.
✓ Mixed system.

Due to the development of modern technology, the system for ensuring cyber security requires the participation and close cooperation of telecommunication and information technology organizations, academic institutes, universities, individuals, and legal entities, in addition to organizations with special functions to ensure security.

Summarizing the experiences of the countries surveyed:

✓ It is standard to update the cyber security system in a short period of time, i.e., 4 years, mainly to reflect the cyber security strategy.

[1] Xu Longdi, Cyberspace Security: Trends, Conflicts and Strategic Stability, 10 Nov 2017.

✓ When forming the legal framework, the principle of creating regulations appropriate to the specifics of each industry is followed, not by a single law but by a set of laws.

✓ Every sector and every organization shall have the opportunity to perform its main functions in Cyberspace.

✓ When forming the national cyberspace protection system, it is formed in accordance with the national security system, consistent with the characteristics of the national security structure of the country.

✓ 24/7 monitoring of the national cyberspace is conducted, operating a joint team of organizations with special forces and technological organizations.

✓ There is the creation of cyber diplomacy.

✓ A mechanism is created for controlling the organization and its management, which is the main player in the cyber security system.

✓ The National Security Council is the head of the country's cyber security system.

✓ A policy is established to limit the involvement of intelligence agencies as much as possible.

It has become a reality that world political policy and international relations depend not only on the capabilities of the military but also on the capabilities of cyber weapons. Mongolia is on the same level as, and in some indicators surpasses, even developed countries in the use of modern information and communication technology. However, there is a common mistake of neglecting the issue of cyber security when introducing the use of information and communication technology. According to the statistics of the international research organization, the number of cyberattacks recorded in our country is 8 times higher than the world average. In 2023, Mongolia was ranked 137th among countries in the world in terms of having no cyber security policy, no protection of digital information, no cyber army, and no independent cyber security institute, according to the Cyber Security Index[1]. Also, in the annual security situation report issued by the anti-malware software developer Checkpoint, Mongolia ranked first in 2021 in the list of 190 countries 'affected by malicious code'.[2]

Some issues of Syber Security in Mongolia.

Furthermore, the results of the risk assessment carried out in our state-owned organizations show that we do not implement our laws, do not take sufficient action to ensure cyber security, and have not learned to spend money on cyber security.

Reasons for the lack of cyber security in Mongolia include:

✓ The cyber security legal framework has been lacking for many years.

✓ There was no unified organization in the field of prevention, protection, and cooperation against cyberattacks and violations throughout Mongolia.

✓ Many public and private organizations do not conduct cybersecurity risk assessments and fail to identify vulnerabilities in information systems.

✓ Due to the lack of basic knowledge about cyber security, people continue to infect their computers and other equipment with malicious code.

✓ There is no unified policy and planning for the development and qualification of qualified human resources at the national level.

✓ There is a limited ability to identify and defend against targeted attacks by foreign countries.

National cyber security structure of Mongolia.

Within the framework of Mongolia's long-term development policy 'Vision-2050,' the action program to be implemented in 2021-2030, the 'Cyber Security' law with the four laws passed in 2021, and the 'Armed Forces' law are creating a cyber security legal environment in Mongolia. (See the figure 1).

[1] https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1

[2] https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/

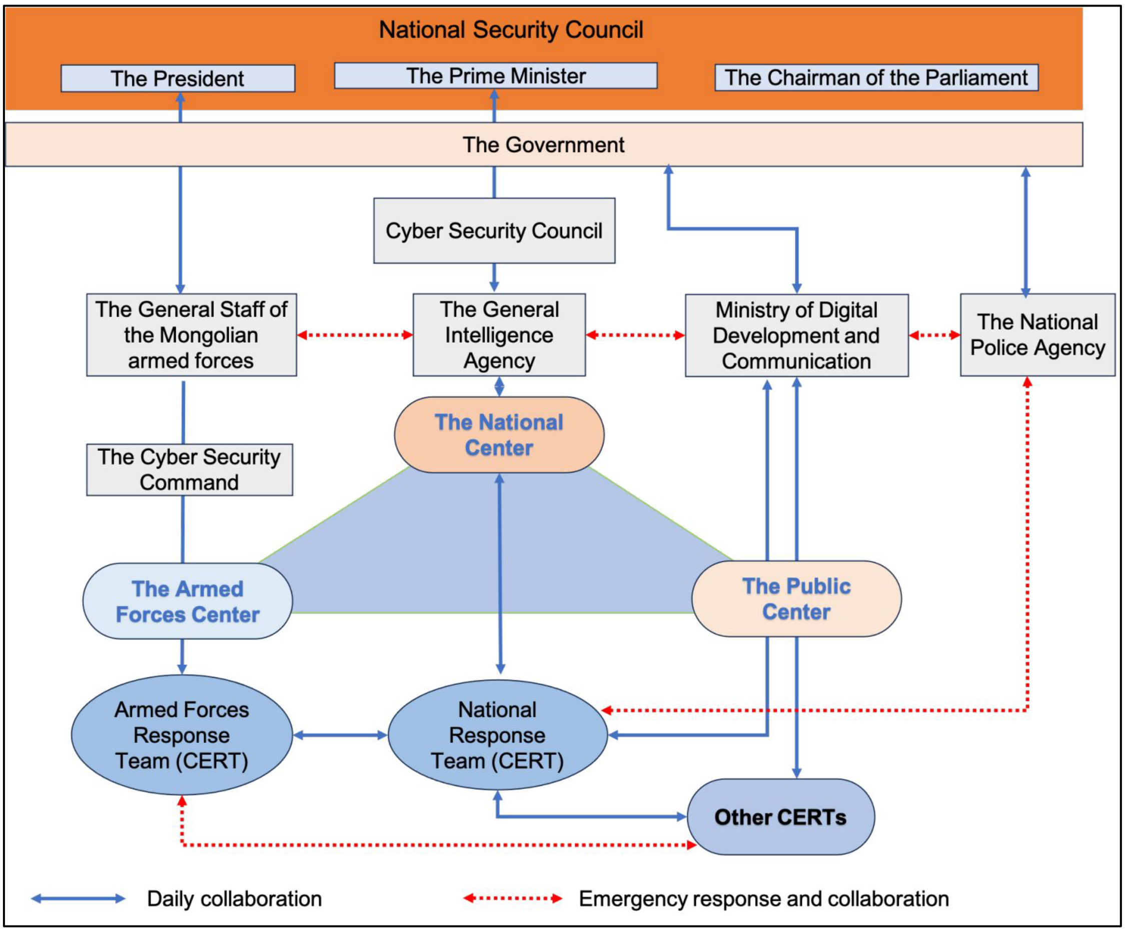
National Security Council
The President
The Prime Minister
The Chairman of the Parliament
The Government
Cyber Security Council
The General Staff of the Mongolian armed forces
The General Intelligence Agency
Ministry of Digital Development and Communication
The National Police Agency
The National Center
The Cyber Security Command
The Armed Forces Center
The Public Center
Armed Forces Response Team (CERT)
National Response Team (CERT)
Other CERTs
Daily collaboration
Emergency response and collaboration

Figure 1. National cyber security structure of Mongolia.[1]

The achievements of the national cyber security system established by the primary law of "Cyber Security" include:

1. The fact that Mongolia has not been able to form its legal environment for many years has provided the opportunity to study international experiences and create a system to ensure national cyber security. Attempts have been made to form a "complex" system for protecting cyberspace with a single law, which specified the areas of responsibility for the organizations involved.
2. For many years, Mongolia has been unable to control its cyberspace. The law now provides for 24/7 continuous monitoring of the state's cyberspace within the National CERT, overseen by the General Intelligence Agency, to establish and operate a joint team to combat cyberattacks and violations, with representatives from the Ministry of Digital Development and Communications, the General Staff of the Mongolian Armed Forces, the National Police Agency, and some telecommunications companies.
3. The armed forces are responsible for defending the country's cyberspace. The organization's activities are divided into two parts, depending on the situation:

✓ When the country is in a state of war: Clause 23.1 of the "Law of Communications" states, "In the event of a state of emergency or war, emergency or force majeure in Mongolia, the communication network shall be mobilized in accordance with the law." Based on this, the Armed Forces are tasked with providing integrated management of defense activities for the information and communication infrastructure, or cyberspace, of Mongolia, organizing cyber operations, and allocating cyber resources to detect, stop, and respond to cyberattacks.

✓ In peacetime: Clause 6.2.12 of the “Law of Armed Forces" its main functions, the armed forces protect the country from external cyberattacks in peacetime, and in Clause 14.1.2 of the “Law of Cyber Security" the cyber security unit of the Armed Forces "to ensure cyber security of defense

[1] https://www.parliament.mn/nn/16476/

operations, the security of information systems and information networks of the armed forces, and to support operations to ensure the security of the national cyberspace when necessary in peacetime;" duties have been assigned.

The Armed Forces will develop the country's cyberspace defense capabilities, with a focus on both defensive and offensive strategies. Notably, cyberattacks and aggressions are typically conducted and concluded during peacetime.[1] According to the aforementioned law, the Armed Forces are permitted to engage in offensive and defensive activities to protect the country's cyberspace from external attacks.

The primary "Cyber Security" law mandates the establishment of a Cyber Security Council, chaired by the Prime Minister, as part of the mechanism for ongoing monitoring to ensure cyber security operations. According to the "Cyber Security" law, the defense of Mongolia's cyberspace is divided into the following four main parts:

✓ The Armed Forces have been assigned the responsibility of protecting against external cyberattacks that threaten the country's security. Therefore, they will be responsible for the protection and investigation of external cyberattacks against the sovereignty of the state.

✓ The task of ensuring the cyber security of state institutions and critical infrastructure has been assigned to the General Intelligence Agency (GIA). Consequently, the GIA is responsible for investigating cyberattacks and malicious code targeting these organizations.

✓ The Ministry of Digital Development and Communication is charged with the state's cyber security policy and regulation, and it is committed to ensuring the cyber security of public organizations and private critical infrastructure organizations.

✓ The police are tasked with the investigation of cybercrimes.

The critical aspects of the state cyber security system created by the primary "Law of Cyber Security" include:

✓ In most countries, the National Security Council is the governing body for the country's cyber security system. The law stipulates that Mongolia's cyber security system will be implemented within the national security framework but does not specify how to participate in various issues.

✓ The law has created a cyber security structure based on the intelligence agency. However, the main role of the intelligence organization is to gather and analyze information, which is not aligned with the fundamental mission of providing cyber security. Consequently, many countries experience internal conflict over this issue, such as South Korea. The primary reason South Korea has not passed the "Cyber Security" law for approximately 18 years is the disagreement among legislators about assigning the cyber security task to the Intelligence Agency. In Mongolia, trust in the intelligence agency by the people and the government has significantly eroded, as evidenced by the agency's strong resistance to assuming responsibility for cyber security during the law's discussion, expressing disbelief and critiquing the law's provisions.

✓ It is inappropriate for the Ministry of Information and Communication Development, as the central state administrative organization, to be tasked with ensuring the cyber security of public and private organizations with sensitive infrastructures. Since this ministry does not have a specific national security mandate, it should not be included in the national security system for carrying out security-related activities.

✓ The role of financial institutions is not addressed in the law. Cyber security operations require sophisticated hardware and software, necessitating considerable financial resources. Nevertheless, the law neglects the responsibilities of the central government administration organization that oversees financial matters, including the state's finances and monetary policy.

Four years have passed since the Cyber Security Law was enacted, and Mongolia's cyber security system was established. However, Mongolia's cyber security has not shown improvement. According to the cyber security index issued by the International Telecommunication Organization, Mongolia was ranked 129th when the law was passed in 2020, but its ranking fell to 137th by 2023.

Therefore, amending the 'Cyber Security Law' to reform Mongolia's national cyber security structure is necessary. In line with global trends, these changes should aim to diminish the roles of the Intelligence Agency and the Ministry of Electronic Development and Communication, which currently spearhead Mongolia's national cyber security efforts.

[1] Ian Traynor (17 May 2007). "Russia accused of unleashing cyberwar to disable Estonia". The Guardian, *arch 2022.* Retrieved 17 November 2020. *Markoff, John (12 August 2008).* "Before the Gunfire, Cyberattacks". *The New York Times.* Archived *from the original on 30 March 2019.* Retrieved 21 February 2017.

Other applicable laws include:

- ✓ The Law of Mongolia on State and Official Secrets, enacted on December 1, 2016 'the State Secrets Law;
- ✓ the Civil Code of Mongolia, enacted on January 10, 2002 the Civil Code;
- ✓ the Criminal Code of Mongolia, enacted on December 3, 2015 'the Criminal Code'; and
- ✓ the Law of Mongolia on Minor Offences, enacted on May 11, 2017 'the Minor Offences

The Cyber Security Law is another important law related to ensuring the integrity, confidentiality, and accessibility of data in the cyber environment. With the adoption of the law, a system and legal framework for ensuring cybersecurity have been formed, the rights and obligations of citizens, legal entities, and government organizations regarding cybersecurity have become clearer, and activities to ensure cybersecurity, to conduct a cybersecurity risk assessment, and to audit and monitor data security, and to provide integrated management and arrangement have been brought into force.

CONCLUSION.

The key provisions and developments under the Cyber Security Law are: the obligations of legal entities providing information technology services in the field of information processing, storage, distribution, and electronic computing, and ensuring its normal functioning through a shared information system in the cyber environment are defined and have obligations to:

- ✓ approve internal procedures for ensuring cybersecurity;
- ✓ immediately report a cyber-attack to the respective center for combating cyber-attacks and breaches and seek assistance if it cannot be stopped;
- ✓ keep information system operation records for the period specified in the common cybersecurity regulation;
- ✓ obtain professional and methodological assistance from relevant government organizations and cooperate with them in the activities of ensuring cybersecurity;
- ✓ have a unit or an official responsible for ensuring cybersecurity;
- ✓ perform a cybersecurity risk assessment every two years, whenever the conditions and situations specified in the relevant regulations arise, and take necessary measures;
- ✓ conduct an information security audit every year, whenever the conditions and situations specified in the relevant regulations arise, and take necessary measures according to the findings, recommendations, and requirements issued;
- ✓ conduct relevant cybersecurity checks for newly introduced IT products and services and their changes and updates;
- ✓ notify users affected by cyber-attacks and violations immediately;

By improving the legal framework for cyber security, creating a unified management system, ensuring cyber security of critical information infrastructure, improving flexibility, improving public awareness of cyber security, improving human resource capabilities, and developing external and internal cooperation.

This strategy aims to ensure the security, privacy, and availability of information in the cyber environment at the national level.

- ✓ Strengthening the legal framework for cyber security
- ✓ Ensuring the cyber security of organizations with critical information infrastructure
- ✓ Improvement of human resource capacity, new training, and retraining
- ✓ Expand cooperation to ensure cyber security
- ✓ Building cyber security resilience and attack response capabilities

The implementation of the national strategy will be provided by the Government and the National Cyber Security Council under joint management and coordination.[1]

REFERENCES

1. https://legalinfo.mn/mn/detail?lawId=16390365491061.
2. https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1.

[1] https://cscouncil.gov.mn/en/strategic-objective

3. https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/.
4. *Ian Traynor (17 May 2007). "Russia accused of unleashing cyberwar to disable Estonia". The Guardian, arch 2022. Retrieved 17 November 2020. Markoff, John (12 August 2008). "Before the Gunfire, Cyberattacks". The New York Times. Archived from the original on 30 March 2019. Retrieved 21 February 2017.*
5. https://cscouncil.gov.mn/en/strategic-objective.
6. https://www.parliament.mn/nn/16476/.
7. “Mongolia Data Protection Overview”, April 2024, https://www.dataguidance.com/notes/mongolia-data-protection-overview#:~:text=With%20the%20adoption%20of%20the,conduct%20a%20cybersecurity%20risk%20assessment%2C.
8. https://legalinfo.mn/mn/detail?lawId=16532522757001.
9. https://en.micoa.mn/post/131381.
10. Xu Longdi, Cyberspace Security: Trends, Conflicts and Strategic Stability, 10 Nov 2017.