An In-Depth Study For A Proposed National Cyber Security Strategy For Digital Economy In Alegria

Sereir El Hirtsi Hayet
Blida 2 University, Laboratory Of Economic And Human Development In Algeria, Algeria

h.sereir-elhirtsi@univ-blida2.dz

Reçu le : 15/10/2023 **Accepté le :** 10/12/2023 **Publié le :** 31/12/2023

Abstract:

This study aims to analyze the national cybersecurity strategies for eighteen countries, in terms of concept, vision, objectives, principles, and main action plans at the operational level. In addition, this study seeks to provide a proposed vision for a national strategy for cybersecurity that focuses on supporting the digital economy in Algeria.

The study concluded that to achieve this vision, a strategy must first be formulated that makes cybersecurity a key factor in protecting the digital economy and society. This strategy should focus on improving information security systems, providing high-tech technology for cybersecurity purposes, and building the capabilities of human resources in this field, in addition to developing the judicial and security system and making it in line with international developments.

Keywords: National Cybersecurity Strategies; Digital Economy; Cyberthreats; Algeria.
Jel Classification Codes : F44; O33; D8; C18.

ملخص:

تهدف هذه الدراسة إلى تحليل الاستراتيجيات الوطنية للأمن السيبراني لثمانية عشر دولة، من حيث المفهوم، الرؤية، الأهداف، المبادئ وخطط العمل الرئيسية على المستوى التشغيلي. بالإضافة إلى ذلك، تسعى هذه الدراسة إلى تقديم رؤية مقترحة لاستراتيجية وطنية للأمن السيبراني تركز على دعم الاقتصاد الرقمي في الجزائر.

وخلصت الدراسة إلى أنه لتحقيق هذه الرؤية لا بد أولاً من صياغة استراتيجية تجعل من الأمن السيبراني عاملاً أساسياً في حماية الاقتصاد والمجتمع الرقمي. وينبغي أن تركز هذه الاستراتيجية على تحسين أنظمة أمن المعلومات، وتوفير تكنولوجيا عالية التقنية لأغراض الأمن السيبراني وبناء قدرات الموارد البشرية، بالإضافة إلى تطوير المنظومة القضائية والأمنية وجعلها تتماشى مع التطورات الدولية.

الكلمات المفتاح : الاستراتيجيات الوطنية للأمن السيبراني؛ الاقتصاد الرقمي؛ التهديدات السيبرانية؛ الجزائر.
تصنيف JEL : F44; O33 ; D8; C18 .

Auteur correspondant : Sereir El Hirtsi Hayet, Email: h.sereir-elhirtsi@univ-blida2.dz

I. Introduction:

The global economy has undergone a massive and accelerating digital transformation, creating new business models, innovative products, and services, Digital information technology has replaced devices, and data has become a valuable currency in this new digital era. However, the focus is increasingly shifting from the economic benefits to the risks arising from the use of information and communications technology (ICT), namely cyber security risks.

Cybersecurity is a new field of security study that is not fully understood in terms of its nature, dimensions, trends in occurrence, and other issues related to it, and this explains the difficulty of dealing with it. Cybersecurity mainly includes information classification, data integrity and confidentiality permissions, defense, devices, services, networks, and control systems including physical, technical, procedural, and legal. Cybersecurity is also mainly concerned with cyber attacks.

Cyber attacks have increased significantly, as the second quarter of 2023 saw an 8% surge in global weekly cyberattacks, with organizations facing an average of 1258 attacks per week (GPT, 2023), The prediction is that $8 trillion will be lost to cyber crimes by the end of 2023, which is almost a third of the USA's GDP in 2022 and twice as much as India's predicted GDP in March 2023. The global loss to cybercrime will grow more than 15% year by year to reach $10.5 trillion by 2025 (James, 2023).

Algeria has not been spared cybercrimes and attacks, as the number of crimes jumped from 2,838 in 2021 to 4,600 in 2022, while 500 cybercrimes have been recorded since the beginning of 2023 (Bashoush, 2023) . Kaspersky also ranked Algeria third in the world in terms of countries in which users faced the greatest risks of infection via the Internet in 2023 (Kaspersky, 2023).

To address these challenges, Algeria needs to develop a national cyber security strategy (NCSS) that aims to build a secure, reliable, and resilient cyberspace while promoting the prosperity of the digital economy and the well-being of its citizens. Accordingly, this study seeks to answer the following problem: **What is the appropriate vision for building a national strategy for cybersecurity in Algeria that supports the digital economy?**

The importance of this study lies in the importance of the issue of cybersecurity, which has become one of the most essential pillars of the digital economy in the world. Therefore, this study focuses on analyzing national strategies for cyber security in some foreign and Arab countries to provide a proposed vision of a national strategy for cyber security that supports the digital economy in Algeria.

II. Literature Review :

In this section, the opinions of relevant previous studies on the subject of the study are examined and discussed.

The (Luiijf & et al, 2013) aimed to analyze the NCSS in ten countries (Australia, Canada, Czech Republic, France, Germany, Japan, Netherlands, New Zealand, United Kingdom, and United States). Make comparisons and identify differences. The study concluded that the significant differences in NCSS stem from differences in some points: economics, national security, or military defense. Moreover, the main difference lies in the scope of cybersecurity: Internet-only systems versus the entire ICT. The study also found that most national security systems lack a comprehensive approach to dealing with threats to cyberspace.

The (Riza & et al, 2016) study sought to identify common drivers that enable an understanding of the development of NCSS as a public policy phenomenon. To achieve this, the paper uses qualitative coding for the NCSS review of 54 countries. The study identified a wide range of motivations that led to the creation of the NCSS. Interestingly, these motives include more than just national protection in cyberspace, but also political will. Furthermore, the study confirmed that for the vast majority of countries, establishing an (NCSS) supports national security by countering cyber threats, protecting state secrets, enhancing national resilience, or enhancing economic security. The study also found that enhancing national security in cyberspace requires

governments to deal with the nature of Internet technologies. This requires more than just dealing with currently known vulnerabilities, but also taking into account future innovations in cyberspace.

While, the (Chooi & Ahmad, 2017) study sought to gain insights into the relationship between the development of the NCSS National Cybersecurity Strategy and the success of the nation's digital economy based on literature from journal articles, global reports, current industry events, and market trends. Where the study attempted to analyze the National Statistics Center in nine countries on the success of the digital economy. Interestingly, it was found that the nation's willingness to foster a digital economy is not related to the development and dissemination of the nation's NCSS. Although the study demonstrated the importance of cybersecurity to protect and enable the digital economy. Moreover, the study showed that countries with high digital trust rely less on NCSS at the national level to enhance trust in the digital space, but the study completely neglected the reasons that led to this.

Also, (Kaushik & et al, 2019) Study aimed to assess the strength of the current cybersecurity strategy in Bangladesh compared to some of the most technologically advanced countries in the Asian continent and other than the USA, Japan, Singapore, Malaysia, and India. Moreover, the study made suggestions for the modernization of NCSS in Bangladesh. The study found the strategy to be reasonably robust in promoting cybersecurity education, ongoing risk assessments, and anti-cybercrime policy. However, some major improvements are needed in research and development, coordination with international law, and balancing cybersecurity with civil liberties and regional cooperation.

Previous studies provided an analysis of the national strategy for cybersecurity in some countries, but this study seeks to build a proposed vision for a national strategy for cybersecurity to protect the digital economy in Algeria.

III.Method and Approach :

This study examined the literature of publicly available documents. The framework for the comparison was based on the Global Cybersecurity Index (NCSI, 2023). In addition, the study used the ITU guide (ITU, 2018). to provide extensive research into the various aspects of NCSS. The data set includes NCSSs published in English across eighteen nations. The main themes sought to be explored are the definition of Cyber security; Strategic vision and timeframe; Strategic objectives; Guiding principles; Main Action Plans at the Operational Level; Responsible agency; and cooperation measures.

Furthermore, for this research, the NCSSs for this study were selected from the 2023 normalized score of the GCI of the most committed countries to cybersecurity. Table 1 shows the GCI ranking of the selected countries :

Table 1: Selected countries based on Global Cybersecurity Index (GCI)

Rankine	Country	Rankine	Country
1	The United States of America (USA)	8	Canada (CAN)
2	Kingdom of Saudi Arabia (KSA)	9	France
3	Estonia	10	India (IND)
4	Spain (ESP),South Korea (KOR), Singapore (SGP)	11	Turkey (TUR)
5	Malaysia (MAS) , United Arab Emirates (UAE)	12	Australia (AUS)
6	Lithuania	13	Germany (GER)
7	Japan (JPN)		

Source : (NCSI, 2023).

Although Estonia, Lithuania, and France occupy good positions in the classification, they were excluded from the comparative analysis due to insufficient information. However, Egypt (EGY), Qatar (QAT), Tunisia (TUN), and Iraq (IRQ) were added to increase the number of Arab countries studied, and we also added China (CHN) as an economic power.

IV. Analysis Of National Strategies For Cybersecurity :

The National Cybersecurity Strategy (NCSS) is the main document of nation states to set strategic principles, guidelines, and objectives, and in some cases specific measures in order to mitigate risk associated with cybersecurity (ENISA, 2023). Also, The national cybersecurity strategy (NCSS) indicates "a careful plan or method of protection both informational and non-informational assets through the ICT infrastructure for achieving particular national goals usually over a long period of time" (Riza & et al, 2016, p. 02).

IV.1. Opinions on Cyber Security Strategies :

Through an analysis of the national cybersecurity strategies (NCSS) of 18 countries, considering that each country has different cultural, legal, and political backgrounds, there is a difference between the strategies, but there is general agreement about the form and elements included in the most of strategies, which included: an executive summary; an introduction; Vision; The relationship of the (NCSS) to other strategies at the national and international levels; strategic goals; guiding principles; outline of tactical action; A glossary that includes a harmonized set of international definitions. Most of the strategies focused on key points such as national security; Economy; digital economy; society; military defense; and the international community.

Most of these strategies initially addressed the definition of cybersecurity and cyberspace and its importance, but since countries lack coordinated cyber terminology, they may face obstacles in cooperatively addressing global threats in cyberspace. Moreover, countries have a different understanding of the scope of what cybersecurity is supposed to cover: systems connected to the Internet only or all ICTs. Since some countries are adopting an Internet security approach, they have inadvertently neglected the protection of the offline ICT domains (until now).

Also, most of these strategies dealt with cyber threats and international challenges. However, the strategies are relatively weak when describing detailed action plans under the theme of "international cooperation", international topics such as coordination of activities, dissemination of unified international standards, collaborative strengthening of the international response to cybercrime and other threats, and Tracking down cyber criminals. these topics are not on the priority lists of the strategies.

Most strategies recognize the need for a community-wide approach: citizens, businesses, the public sector, and government. However, the range of actions targeting citizens is often limited to awareness campaigns and information security education in schools. Only some countries have an outreach program that supports citizens with national cybersecurity tools, and Internet Service Providers (ISPs) and the Center for Internet Security (CIS) play a major role in this.

IV.2. Cyber Security Definition :

Table 1 presents an overview of the various definitions and descriptive understandings of 'Cyber Security' in the various NCSS. Only eight nations define 'Cyber Security'.As for the rest of the countries, they implicitly referred to cyber security. It can be observed that some nations focus on the information security aspects whereas other nations consider Cyber Security as a property to address and counter threats from cyberspace. Moreover, there is no harmonized understanding of 'Cyber Security' by the eighteen nations.

Table 2: NCSS definitions of Cyber Security.

USA	References to 'information security' (WH, 2018).
CHN	References to 'intelligence activities during emergencies and political warfare during peacetime' (Netcom, 2016).
IND	Cyber security is the activity of protecting information and information systems (networks, computers, databases, data centers, and applications) with appropriate procedural and technological security measures (DSCI, 2013).
JPN	References to 'the network-based vigilance and monitoring of malicious activities against information systems of administrative organs; fact-finding on the cause of incidents and audit of relevant governmental bodies' (GOJP, 2015).
KOR	References to 'creating an open and safe online environment, and swiftly detecting and blocking cyber threats to guarantee that critical operations of the government continue' (NSO, 2019).
CAN	Cyber security is The protection of digital information, as well as the integrity of the infrastructure and transmission of digital information. More specifically, cyber security includes the body of technologies, processes, practices, and response and mitigation measures designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access to ensure confidentiality, integrity, and availability (PSC, 2018).
AUS	Cyber security is measures relating to the confidentiality, availability, and integrity of information that is processed, stored, and communicated by electronic or similar means (CA, 2020).
GER	Cyber security is the desired objective of the IT security situation, in which the risk of cyberspace has been reduced to an acceptable minimum. (FMIBC, 2021).
ESP	References to 'secure use of networks and information systems by enhancing capabilities to prevent, detect and respond to cyberattacks' (NSC, 2019).
MAS	References to **'**fortifying local capabilities to predict, detect, deter, and respond to cyber threats, nurturing competent people, and deploying effective technologies' (MNSC, 2020).
SGP	References to **'**Safeguard cyberspace activities, and Secure digital infrastructure, devices, and applications that power the digital economy' (CSAS, 2021).
TUR	Cyber security is the protection of information systems forming cyberspace from attacks, assuring confidentiality, integrity, and availability of information/data processed in this environment, detection of attacks and cyber security incidents, and activation of counter-response mechanisms (MTMC, 2016).
UAE	References to 'information security, and protect systems, networks, and programs from digital attacks' (TRA, 2019).
KSA	References to 'secured networks, information technology, operational technology systems, and related hardware and software components, thus protecting services and data from penetration, disruption, modification, entry, use, or exploitation. By doing so, the critical technical linkages between government services and critical national infrastructure are secured and the growth of the Kingdom's digital economy is supported' (NCSA, 2020).
QAT	Cyber security is the set of security tools, policies, concepts and procedures, guidelines, risk management methodologies, procedures, training, best practices, security methods, and technologies that can be used to protect the cyberspace environment and the assets of companies and users (MCIT, 2014).
IRQ	Cybersecurity is the provision of security for critical information infrastructure and other critical elements of the information system (NSA, 2020).
EGY	References to 'Protecting the security of cyberspace and securing the communications and information technology infrastructure, systems, databases, national information, government service portals, and government websites on the Internet' (ESCC, 2017).

TUN	Cybersecurity is the provision of capabilities necessary to protect cyberspace against threats that may affect the confidentiality, integrity, and availability of data and services (NAIS, 2020).

Most strategies share a definition of cybersecurity as the protection of hardware, systems, and software associated with all services, transactions, and information/data provided through information and communication technologies that constitute the national cyberspace.

IV.3.National Cyber Security Visions :

Most National Cyber Security Strategies (NCSS) clearly define the vision. The following table shows the vision for each country:

Table 3 :The national visions on cybersecurity.

USA	Engage Americans and enable them to secure the parts of cyberspace that they own, manage, control, or interact with (WH, 2018).
CHN	Community of a common destiny in cyberspace (Netcom, 2016).
IND	ensure a secure, reliable, resilient and vibrant cyberspace for the prosperity of our nation (DSCI, 2013).
JPN	The government is responsible for overcoming the risks related to the use of information and communication technology by enhancing the protection of critical infrastructures that support social and economic activities and are closely related to the daily life of the nation, and it is also required to take systematic and immediate actions to ensure national security and effective crisis management (GOJP, 2015)
KOR	Creates free and secure cyberspace to support national security, promote economic prosperity, and contribute to international peace (NSO, 2019)**.**
CAN	Our national plan for making cyberspace more secure for all Canadians (PSC, 2018).
AUS	Maintaining a secure, resilient, and reliable electronic operating environment that supports Australia's national security and maximizes the benefits of the digital economy. A safer online world for Australians and their businesses and the essential services we all depend on (CA, 2020)**.**
GER	providing security in an ever-evolving cyber environment, and promoting economic and social prosperity in Germany (FMIBC, 2021)**.**
ESP	Ensuring the security of Spain, its citizens, and its residents in cyberspac**e** (NSC, 2019)**.**
MAS	Malaysia cyberspace is secured, trusted and resilient, fostering economic prosperity and citizens' well-being (MNSC, 2020) **.**
SGP	strengthening the security and resilience of our digital infrastructure and enabling safer cyberspace to support our digital way of life (CSAS, 2021)**.**
TUR	support the development of the country's economy, the preservation of an integrated life, and the choice of national security; To have a strong cyber environment in our country and become a brand when it comes to cyber security between countries (MTMC, 2016)**.**
UAE	Creating a secure and flexible cyber environment in the country that helps individuals achieve their ambitions and enables companies to develop (TRA, 2019)**.**
KSA	A resilient, secure, and trusted Saudi cyberspace that enables growth and prosperity (NCSA, 2020).
QAT	Creating and promoting a safe electronic space to protect the national interests of the State of Qatar and preserve the basic rights and values of society (MCIT, 2014).

IRQ	A secure, vibrant, resilient, and trusted society that provides opportunities for its citizens, protects national assets and interests, and promotes peaceful interactions and proactive participation in cyberspace for national prosperity **(NSA, 2020)**.
EGY	Information in cyberspace is an essential part of the economy and national security system, and the state is obligated to take the necessary measures to preserve it, in the manner regulated by law (ESCC, 2017)**.**
TUN	Tunisian state is able to prevent cyber threats and withstand them by relying on national capabilities, leading and managing national cyberspace, supporting digital trust, enhancing international cooperation, and achieving leadership in the digital field (NAIS, 2020).

IV.4.Strategic Objectives :

The following table shows the strategic cybersecurity objectives. Most national cybersecurity strategies contain between three and five strategic objectives, which are described as follows:

Table 4 : Strategic objectives.

USA WH, 2018)	1-Prevent cyber attacks against US critical infrastructure. 2- Reduce national vulnerability to cyber attacks. 3- Minimise damage and recovery time from cyber attacks that do occur.
CHN (Netcom, 2016)	Promote peace, security, openness, cooperation, and order in cyberspace, protect national sovereignty, security, and development interests, and achieve the strategic goal of building a cyber force.
IND (DSCI, 2013)	1-To further ICT in India as an engine for economic growth and prosperity. 2-To create a security framework for securing cyberspace.
JPN (GOJP, 2015)	1-Reinforced policy to counter cyber attacks. 2-Policies to adapt to changes in the cyber security environment. 3-Active/dynamic cyber security measures.
KOR (NSO, 2019)	1-Ensuring stable operations of the state. 2- Responding to cyberattacks. 3-Building a strong foundation for cybersecurity.
CAN (PSC, 2018)	Countering the cyber security threat by: 1-Securing government systems 2-Partnership to secure critical electronic systems outside of the federal government 3-Helping Canadians be safe online
AUS (CA, 2020)	1- All Australians are aware of cyber risks, secure their computers, and take steps to protect their identity, privacy, and financial resources online. 2- Australian companies operate and communicate with secure and resilient information on technologies to protect the integrity of their operations and the identity and privacy of their customers. 3- The Australian Government ensures that its information and communications technologies are secure and resilient.
GER (FMIBC, 2021)	1-Define the framework for the cybersecurity activities of the federal government. 2-Create transparency and understandability for all stakeholders. 3-Facilitate the active and meaningful participation of all stakeholders. 4-Taking into account EU specifications. 5-Prepare systematically for future evaluations and continuous revision of the strategy.
ESP	Defend the interests, vital values, and strategy of Spain (NSC, 2019).

MAS (MNSC, 2020)	1-Further improve the national response to cybersecurity. 2-Raising awareness of the impact of cyber incidents on national security. 3-Test the ability of CNII agencies/organizations to deal with cyber incidents.
SGP (CSAS, 2021)	1-Building a cybersecurity ecosystem underpinned by research and innovation for our security and economic needs. 2-Develop and sustain a strong cybersecurity workforce to meet our security and economic needs.
TUR (MTMC, 2016)	1-Ensure the security, confidentiality, and privacy of information. 2- Enhancing cyber security and ensuring higher efficiency in detecting cyber incidents. 3-Develop locally significant technologies and products to ensure cybersecurity, confidentiality, and privacy.
UAE (TRA, 2019)	1-Enhancing the confidence of community members to participate securely in the digital world. 2-Promoting innovation in the field of cybersecurity and consolidating the culture of investment in the field. 3-Enabling small businesses to protect themselves against cyber attacks. 4-Protect sensitive information and state infrastructure. 5-Building a world-class human cadre in the field of cybersecurity in the country
KSA (NCSA, 2020)	1-Unify: Whole-of-Nation Cybersecurity 2-Manage: Adaptive Risk Management 3-Assure: Cyber Ecosystem Assurance 4-Defend: Dynamic Defense 5-Partner: Collaborative Security 6-Build: Cyber Ecosystem Development
QAT (MCIT, 2014)	1- Protecting the national vital information infrastructure. 2- Responding to, resolving, and recovering from cyber incidents and attacks. 3- Developing the legal and regulatory framework to enhance the safety and vitality of cyberspace. 4- Promoting a culture of cybersecurity that supports the safe and appropriate use of cyberspace. 5- Developing national capabilities for cyber security.
IRQ	Provide a coherent roadmap, initiatives, and means to implement and achieve the national vision of cybersecurity (NSA, 2020).
EGY (ESCC, 2017)	Confronting cyber risks and enhancing confidence in the communications and information infrastructure, its applications, and services in various vital sectors and securing them to achieve a safe and reliable digital environment for Egyptian society in its various sectors.
TUN (NAIS, 2020)	1-Leading and Managing the National Cyberspace. 2-Prevention of cyber threats and steadfastness. 3- Support digital trust. 4- Achieving leadership in the digital field. 5- International cooperation.

Despite the differences in wording, most NCSS aim for a safe, secure cyberspace for the citizens, society, and nation.

IV.5.Guiding Principles and Framework Conditions :

The following table shows the guiding principles and framework conditions included in their national strategies, as follows:

Table 5 : Guiding principles and framework conditions.

USA (WH, 2018)	Privacy and civil liberties need to be protected.	**CHN** (Netcom, 2016)	1-Respect and protect the sovereignty of cyberspace. 2-Peaceful use of cyberspace. 3-Cyberspace is governed by law. 4-Network security coordination and development.
SGP (CSAS , 2021)	1-Build Resilient Infrastructure. 2-Enable a Safer Cyberspace. 3-Enhance International Cyber Cooperation.	**CAN** (PSC, 2018)	1-Securing government systems. 2-Partnership to secure vital electronic systems abroad. 3-Helping Canadians to be safer online.
ESP (NSC, 2019)	1-comprehensive approach. 2-coordination. 3-Effective use of resources. 4-Anticipation and prevention. 5- Flexibility. 6- Responsible bonding. 7- Respect for democratic values, human rights, and the rule of law.	**MAS** (MNSC, 2020)	1-Effective Governance and Management. 2-Strengthening the legislative framework and enforcement. 3-Stimulating innovation, technology, research and development, and industry on a global level. 4-Strengthening capacity building, awareness, and education. 5-Strengthening global cooperation.
IND (DSCI , 2013)	1-secure (national cyberspace). 2-Strengthening (structures, people, processes, capabilities). 3-Synergy (resources including collaboration).	**TUR** (MTMC, 2016)	1-Strengthening cyber defense and protecting infrastructure. 2-Combating cybercrime. 3-Improving awareness and human resources. 4-Developing a cyber security ecosystem. 5-Integrating cyber security with national security.
JPN (GOJP , 2015)	1-Ensure the free flow of information. 2-rule of law. 3-openness. 4-independence. 5-Multi-stakeholder collaboration.	**UAE** (TRA, 2019)	1-Cyber security laws and regulations. 2-A vital environment for cyber security. 3-National Cyber Incident Response Plan. 4-Vital Information Infrastructure Protection Program. 5-Partnerships.
KOR (NSO, 2019)	1-Balancing individual rights and cybersecurity. 2-Conducting security activities based on the rule of law. 3-Building a system of sharing and cooperation.	**GER** (FMIBC, 2021)	1-Establishing cyber security as a joint task for government, private industry, the research community, and society. 2-Reinforcing the digital sovereignty of the government, private industry, the research community, and society. 3-Making digital transformation securely. 4-Setting measurable, transparent objectives.

AUS (CA, 2020)	1- National leadership. 2- Shared responsibilities. 3- Partnerships. 4- Active international participation. 5- Risk management. 6- Protecting Australian values.	**QAT** (MCIT, 2014)	1-Government leadership of cyber security efforts. 2-Cyber security is a shared responsibility. 3-Preserving basic rights and values.
IRQ (NSA, 2020)	1-effective government. 2-Legislative and Regulatory Framework. 3-Cyber Security Technology Framework. 4-Cybersecurity culture and capacity building. 5-Research and development towards self-reliance. 6-Compliance and Enforcement. 7-Preparedness for cyber security incidents. 8-International cooperation.	**EGY** (ESCC, 2017)	1-Political, institutional, strategic, and operational support. 2-Legislative, Regulatory, and Implementation Framework. 3-Scientific research and development and development of the cybersecurity industry. 4-Developing human cadres and enhancing the expertise necessary to implement the cybersecurity system. 5-Cooperation with friendly countries and relevant international and regional organizations. 6-Community awareness.
TUN (NAIS , 2020)	1- Strengthening the national cyberspace and protecting sensitive information infrastructures against threats that could affect national security. 2- Developing procedures for dealing with cyber incidents and managing crises related to the field.	**KSA** (NCSA, 2020)	1-Whole-of-Nation Alignment. 2-Centralized Governance, Decentralized Operations. 3-Agile and Future-Focused. 4-Prioritization Based on Risk Level. 5-Cooperation and support. 6-Relying on Saudi Nationals and Investment Opportunities. 7-Setting benchmarks and performance indicators.

Most of the foregoing cybersecurity strategies share three principles that can be formulated as follows:

- Fulfilling all legal and social responsibilities by individuals, institutions, society, and the state in providing cyber security.
- Coordination, joint participation, cooperation, and information exchange between the public sector, the private sector, universities, and non-governmental organizations.

Advanced cooperation in the management of electronic incidents between the international centers for cybersecurity operations

IV.6.Main Action Plans at the Operational Level :

By analyzing countries' national cybersecurity strategies NCSS, all countries have identified tactical action plans and often a set of detailed actions in support of their strategic cybersecurity objectives. Where most NCSSs express an urgent need to take action to achieve their strategic goals. The actions taken can be summarized as follows (WH, 2018) (Netcom, 2016) (DSCI, 2013) (NCSA, 2020) (NSC, 2019) (GOJP, 2015) (NSO, 2019):

- Building a secure electronic system;
- Supporting national cybersecurity technology and programs;
- Establish a National Incident Preparedness and Cyber Security Strategy Center (NISC) that will assume a key and leading role in coordinating the activities of ministries and promoting collaboration between industry, academia, and the public and private sectors;

- Establishing a national inventory of critical infrastructure, meeting the security requirements of critical infrastructure, and supervising it by a competent body;
- Create international standards-compliant legislation that also contains cybersecurity audit standards;
- Improving the regulatory and supervisory awareness and the competencies of the institutions and ministries organizing the sector and others in the field of cybersecurity;
- Protection of information systems in organizations not only from attacks but also from human errors and disasters;
- Upgrading each organization to a level of efficiency in operating its information security management process;
- Raising the level of awareness of executives in the field of cybersecurity;
- Encouraging all organizations, both private and public, to appoint a member of senior management to be responsible for information security (CISO), responsible for cybersecurity efforts and initiatives;
- Ensure that all organizations allocate a specific budget to implement cybersecurity initiatives and to respond to emergencies arising from cyber incidents;
- Training the human resources in the field of cyber security and encouraging individuals, researchers, and students who aim to specialize in this field (FMIBC, 2021);
- Forming a national cybersecurity system to engage and coordinate public institutions, the private sector, NGOs, supervisory institutions, universities, software companies, and all other stakeholders (MNSC, 2020);
- Providing advice to small and medium enterprises to increase their cyber resilience (TRA, 2019);
- Create a culture of secure software development and supply (MTMC, 2016);
- Promote standardization of cyber security, authentication, and certification (CSAS, 2021);
- Encouraging scientific research and development of the cybersecurity industry (PSC, 2018);
- Strengthening international cooperation in cyberspace (CA, 2020).
- Cybersecurity requires the participation of not only governments but also individuals and businesses. On it, governments need to strengthen cooperation open doors to that end, and enhance policy transparency with the ultimate goal of continuously implementing cybersecurity policies based on public trust.

IV.7.Stakeholders in a Cybersecurity Strategy :

In terms of stakeholders, most countries focus their cybersecurity strategy on government, national security, and Internet Security Centers (CIs), others focus on the Internet Service Provider (ISP), and other countries expect their citizens to take an active role in cybersecurity. Other countries such as Germany and the USA explicitly consider global electronic infrastructures to be stakeholders in cybersecurity.

In general, the stakeholders in (NCSS) are state/national security; Citizens; Internet service providers; Internet security centers; technology companies; large organizations; Small and medium-sized companies; and global infrastructure.

IV.8. National Cybersecurity Strategy Institutionalization :

USA delegated cybersecurity to the US Department of Homeland Security (DHS) (WH, 2018), while China established the Cyberspace Administration (CAC) (Netcom, 2016). India has established agencies specializing in cyber security (DSCI, 2013). While South Korea and Spain have authorized the National Security Office in the cyber domain (NSO, 2019) (NSC, 2019).

Japan has established an internal government council "National Incident Preparedness Center and Cyber Security Strategy" (NISC) (GOJP, 2015). Germany has established a Commission (CSC) which is also an intergovernmental council, but private stakeholders are allowed to participate as observers (FMIBC, 2021).

Malaysia has formed the Cyber Security Agency (NACSA), a specialized agency that oversees all national cyber security functions formed under the auspices of the National Security Council (NSC) (MNSC, 2020). Singapore has formed the Singapore Information Technology Security Authority (SITSA), and the Cyber Security Agency (CSA) as the central agency to oversee and coordinate all aspects of cyber security for the nation (CSAS, 2021).

Australia has set up two organizations: CERT Australia, which is responsible for providing cybersecurity information and advice to the Australian community, and Cyber Security Operations Center (CSOC) which is responsible for and analyzes complex cyber-attacks, and assists in responding to cyber incidents across government and private sector critical systems and infrastructure (CA, 2020). (CA, 2020).

Canada has focused on creating a National Cybercrime Coordination Unit (RCMP) to expand its cybercrime investigation capacity, and to establish a focal point for both domestic and international cybersecurity partners (PSC, 2018).

The United Arab Emirates has established the National Cyber Incident Response Committee (NRC) with the mission of making strategic decisions related to the national plan for responding to cyber incidents, and the Cyber Intelligence Unit (CIU) is tasked with enabling intelligence sharing between organizations to improve awareness of cyber threats (TRA, 2019).

The Kingdom of Saudi Arabia established the National Cybersecurity Authority (NCA), and linked it directly to the King, to supervise cybersecurity affairs in the Kingdom and to be the national reference for cybersecurity (NCSA, 2020).

In the national cybersecurity strategies (NCSS), Egypt emphasized the establishment of the Supreme Council for Cybersecurity (ESCC, 2017), Tunisia the Communications and Information Security Committee of the National Security Council (NAIS, 2020), Turkey and Iraq focused only on Cyber Incident Response Teams (CIRT) (MTMC, 2016), and Qatar also established the National Committee for Information Security (MCIT, 2014), Furthermore, most other countries in the NCSS state that they will strengthen their national CERT team if it already exists; Other countries plan to create a national computer emergency team.

V. A Proposed Vision For A National Cybersecurity Strategy To Protect The Digital Economy In Algeria :

Based on the extrapolation of previous studies and national strategies for cyber security in foreign and Arab countries, we came to this vision, which revolves around preparing a national strategy for cyber security to protect the digital economy in Algerian.

We have divided this strategy into five phases as defined by the International Telecommunication Union (ITU) in the Guide to Developing a National Cybersecurity Strategy (ITU, 2018). Also, We have adapted these stages according to the Algerian context. as each stage includes a set of steps and procedures to be taken according to the Algerian environment. These stages are as follows:

V.1.Phase 1: Starting

This phase aims to identify the entity responsible for the strategy, form a steering committee, and creation of a cybersecurity agency. Here is a breakdown of this stage:

Identifying The Authority Responsible for The Strategy	- Appointment of the authority responsible for the strategy by the executive branch. - The strategy should allocate the human, financial, and material resources necessary for its implementation. - The strategy should focus on enhancing and sustaining cybersecurity at the highest level of government. - Identify relevant stakeholders from the government, the private sector, and civil society.

Formation of a Strategy Steering Committee	- Create a steering committee to work with the responsible body in developing the strategy. - Clearly defining the role of the Steering Committee from the start. - Enabling the committee to provide direction, quality assurance, transparency, and inclusiveness in strategy development. - Identify stakeholders who will be involved in preparing the strategy to ensure that all relevant knowledge and experience are used. - Collaborate with ICT companies, critical infrastructure operators, academics, and experts to raise the level of cybersecurity.
Creation of a Cybersecurity Agency	- The strategy should identify the competent agency for cybersecurity at the national level. - This agency clarifies the roles, responsibilities, decision-making, and tasks required to ensure the effective implementation of the strategy. - Provide direction, coordination, and oversight of strategy implementation. - Setting performance targets for various departments, ministerial or governmental institutions, or individuals responsible for specific aspects of the strategy.

V.2.Phase 2: Diagnosis

This stage aims to collect data to assess the national reality of cyber security and to identify current and future cyber risks :

National Cybersecurity Situation Assessment	- The strategy should enable the effective management of cybersecurity risks and flexibly lead economic and social activities. - The strategy should encourage organizations to prioritize their investments in cybersecurity and proactively manage risk. - The strategy should encourage the adoption of business continuity measures, which include incident and crisis management, as well as recovery plans.
Risk Management And Resilience	- The strategy should enable the effective management of cybersecurity risks and flexibly lead economic and social activities. - The strategy should encourage organizations to prioritize their investments in cybersecurity and proactively manage risk. - The strategy should encourage the adoption of business continuity measures, which include incident and crisis management, as well as recovery plans.

V.3.Phase 3: The Stage of Preparing and Publishing the Strategy

This stage aims to develop the text of the strategy through the involvement of key stakeholders from the public sector, the private sector, and civil society. where the authority responsible for the strategy, defines the overall vision and scope of the strategy and also defines the objectives and principles, then asks for official approval and publishes the strategy. The procedures for this stage are:

Formulating A National Cybersecurity Strategy	- Effective communication and coordination between all ministries and government agencies and being aware of each other's responsibilities and tasks. - Involve the public sector, the private sector, and civil society through a series of public consultations and working groups.

	- Hold periodic meetings that include all relevant stakeholders in the work plans which are jointly reviewed. - The strategy should reflect the role of government, the private sector, and stakeholders in ensuring cybersecurity. - The strategy should explain how the government will engage these stakeholders and define their roles and responsibilities.
Stakeholder Involvement	- Involve the public sector, the private sector, and civil society through a series of public consultations and working groups. - Hold periodic meetings that include all relevant stakeholders in the work plans which are jointly reviewed.
Request For Official Approval	The authority responsible for the strategy must ensure that the strategy is formally approved by the executive branch. For example, it can be adopted by parliamentary action or government decree.
Deploying the strategy	- The national cybersecurity strategy should be published and readily available. - Its wide availability will ensure that the general public is aware of the government's cybersecurity priorities and objectives.

V.4.Phase 4: Strategy Implementation

This stage aims to develop the action plan, identify the initiatives that will be implemented, allocate the necessary human and financial resources, and define time frames and metrics. Here is a breakdown of this stage:

Action Plan Development	- The strategy should be accompanied by an implementation plan that sets out in more detail how its strategic objectives will be achieved. - effective implementation plans identify who is responsible for each task and objective, the resources required to implement it over time (short, medium, long term), the processes to be used, and the expected results.
Determine The Initiatives To Be Implemented	- The National Cybersecurity Strategy highlights the government's goals and the results it wishes to achieve across the various focus areas identified in the action plan. - The authority responsible for the strategy, in coordination with relevant stakeholders, must identify the specific initiatives in each focus area that will help achieve those goals. - These initiatives could include (organizing cybersecurity tests, establishing security baselines for critical infrastructures, developing an incident reporting framework, and others). - The timeline and effort required to implement these initiatives should be prioritized according to their importance to ensure that limited resources are utilized appropriately.
Allocate Human And Financial Resources For Implementation	- The strategy should identify the resources allocated and appropriate for the implementation, maintenance, and review of the strategy. - Create a central cybersecurity budget (managed by a central cybersecurity governance mechanism).

Define Timeframes And Metrics	- Develop specific metrics, and KPIs to evaluate each of the initiatives taken, such as whether the country has conducted an awareness campaign on the importance of information sharing, and organized cybersecurity training. - Issuance of basic cybersecurity law and specific timetables for implementation must be set.

V.5.Phase 5: Strategic Monitoring and Evaluation

This stage aims to appoint a body responsible for monitoring and evaluation. This body monitors the implementation of the strategy and ensures that its implementation is carried out by the work plan and specified time frames. as follows:

Designate An Authority Responsible For Monitoring And Evaluation	- Define an independent authority responsible for monitoring and evaluating progress in implementing the strategy. - The authority responsible should ideally participate in monitoring and evaluating the metrics for implementing the strategy, action plan, and associated initiatives. - Monitoring and measuring performance and the successful implementation of the strategy implementation plan should be part of the governance mechanisms put in place by the country.
Evaluate The Results Of The Strategy	- Conduct a periodic evaluation of the results and compare them with the objectives set, to understand whether the objectives of the strategy are being achieved or whether they should be reconsidered.

For the successful implementation of this vision, Algeria must first prepare a strategy that makes cybersecurity a key factor in protecting the economy and society. This strategy should focus on a set of methods that fall within the scope of priorities, such as: appointing a body specialized in cybersecurity, issuing a basic cybersecurity law, creating a central budget for cybersecurity managed by a central cybersecurity governance mechanism, in addition to continuous training of human resources and developing Research and development initiatives in the field of cybersecurity. At a later stage, identifying an independent body responsible for monitoring and evaluating progress in implementing this strategy will allow any implementation challenges to be identified early, which in turn will allow the government to either correct the situation or adapt its plans according to lessons learned in the implementation process.

VI. Conclusion:

In the face of ever-changing cyber threats, Algeria needs to be prepared, more than ever, to protect its national security, sovereignty, and economy. By building an effective National Cyber Security Strategy (NCSS). This strategy will play its role in providing guidance and coordination in the field of cyber security while keeping abreast of current and emerging cyber threats and the development of new technologies. All necessary steps will be taken to ensure that threat information is easily accessible and shared among government agencies, businesses, and the general public. The (NCSS) will also provide advice on risks and actions to mitigate them.

Moreover, It is appropriate for Algeria to set rules, standards, and expectations on all elements and entities under its control and responsibility to ensure a safe and secure cyberspace; and cooperation with trusted parties from the international community who share the same goal and ambition. For all of these to happen, Algeria needs a class of competence, capacity, and awareness that can truly protect the national cyberspace, its vital sectors, businesses, and, most importantly, protect its digital economy and the well-being of its citizens, not only from external threats but also from within. It also should focus on the main challenges:

- Digital literacy for Algerian citizens.
- Securing critical infrastructure and governmental networks.
- Keeping up with a changing technological environment.

- Supporting small institutions in their digital transformation.
- Providing protection for small and medium enterprises from cyber threats.
- Encouraging investment in cyber security.
- Qualifying human resources in the field of cyber security.
- Establishing business incubators whose mission is to provide support to companies.
- Opening university majors in the field of cybersecurity.
- Enact deterrent laws for cybercrime, especially those related to electronic commerce.
- conduct an annual cybersecurity audit to identify risks.
- Encouraging cooperation between the public and private sectors in the field of cybersecurity.
- Encouraging research and development of cybersecurity.
- Strengthening international cooperation in the field of cybersecurity.

Referrals and references:

1. Bashoush, N. (2023, 7 07). alshuruq. Récupéré sur Cybercrime: The perpetrators' new weapons to hit people and the economy: https://www.echoroukonline.com
2. CA. (2020). Australia's Cyber Security Strategy 2020. Récupéré sur Commonwealth of Australia: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf
3. Chooi, S. T., & Ahmad, K. M. (2017). National Cyber Security Strategies. Journal of Theoretical and Applied Information Technology,Vol.95. No 23.
4. CSAS. (2021). The Singapore Cybersecurity Strategy. Récupéré sur Cyber Security Agency of Singapore: https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021
5. DSCI. (2013). National Cyber Security Strategy. Récupéré sur Data Security Council of India: https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf
6. ENISA. (2023, 7 6). National Cybersecurity Strategies Guidelines & tools. Récupéré sur The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools
7. ESCC. (2017). Egypt's National Cybersecurity Strategy (2017-2021). Récupéré sur Egyptian Supreme Cybersecurity Council : https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/EgyptNational%20Cybersecurity%20Strategy-English%20version-18%20Nov%202018.pdf
8. FMIBC. (2021). Cyber Security Strategy for Germany. Récupéré sur Federal Ministry of the Interior, Building and Community: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for germany2021.pdf;jsessionid=83773BF1E26409C4CBF6D70599C22DB5.1_cid287?__blob=publicationFile&v=4
9. GOJP. (2015). Japan's Cybersecurity Strategy. Récupéré sur The Government of Japan: https://www.nisc.go.jp/eng/pdf/cs-strategy-en-pamphlet.pdf
10. GPT. (2023, 8 10). Average Weekly Global Cyberattacks peak with the highest number in 2 years, marking an 8% growth year over year, according to Check Point Research. Récupéré sur Check Point : https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/
11. ITU. (2018). Guide to Developing a National Cybersecurity Strategy . Switzerland: Geneva.
12. James, N. (2023, 8 10). Recent Cyber Attacks – 2023. Récupéré sur ASTRA IT: https://www.getastra.com/blog/security-audit/recent-cyber-attacks/
13. Kaspersky. (2023, 7 6). IT threat evolution in Q1 2023. Non-mobile statistics. Récupéré sur Kaspersky Security Network: https://securelist.com/it-threat-evolution-q1-2023-pc-statistics/109917/
14. Kaushik, S., & et al. (2019). A COMPARATIVE ANALYSIS OF THE CYBER SECURITY STRATEGY OF BANGLADESH. International Journal on Cybernetics & Informatics (IJCI) Vol. 8, No.2.
15. Luiijf, E., & et al. (2013). Ten National Cyber Security Strategies: A Comparison. Springer-Verlag Berlin Heidelberg .

16. MCIT. (2014). Qatar National Cyber Security Strategy. Récupéré sur Ministry of Communication and Information Technology: https://nsarchive.gwu.edu/sites/default/files/documents/3903662/Qatari-Government-Qatar-National-Cyber-Security.pdf
17. MNSC. (2020). Malaysia Cyber Security Strategy (22020-2024). Récupéré sur Malaysian National Security Council: https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf
18. MTMC. (2016). National Cyber Security Strategy (2016-2019). Récupéré sur Ministry of Transport, Maritime and Communications : https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/%282%29%20TUR%202016-2019%20NCSS.pdf
19. NAIS. (2020). Cyber security strategy. Récupéré sur National Agency for Information Security (2020-2025): https://ncss.ansi.tn/
20. NCSA. (2020). National Cybersecurity Strategy. Récupéré sur National Cyber Security Authority: https://nca.gov.sa/national_cybersecurity_strategy-en.pdf
21. NCSI. (2023, 7 10). National Cyber Security Index. Récupéré sur e-Governance Academy : https://ncsi.ega.ee/ncsi-index/
22. Netcom, C. (2016). National Cyber Security Strategy. Récupéré sur People's Daily Online: http://politics.people.com.cn/n1/2016/1227/c1001-28980829.html
23. NSA. (2020). Iraqi cyber security strategy. Récupéré sur National Security Advisory: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf
24. NSC. (2019). National Cybersecurity Strategy. Récupéré sur National Security Council: https://www.ccn-cert.cni.es/pdf/documentos-publicos/3812-national-cybersecurity-strategy-2019/file.html
25. NSO. (2019). National Cybersecurity Strategy. Récupéré sur National Security Office: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf
26. PSC. (2018). National Cyber Security Action Plan (2019-2024). Récupéré sur https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf
27. Riza, A., & et al. (2016). Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy. Australasian Conference on Information Systems,Wollongong.
28. TRA. (2019). National Cybersecurity Strategy. Récupéré sur Telecommunications Regulatory Authority: https://tdra.gov.ae/userfiles/assets/Lw3seRUaIMd.pdf
29. WH. (2018). National Cyber Security Strategic of the United States of America. Récupéré sur THE WHITE HOUSE: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf