: https://doi.org/10.25130/tjfps.v1i42.544

P-ISSN: 2312-6639
E-ISSN: 2669-9203

TJFPS
http://tjfps.tu.edu.iq/index.php/politic/index
Tikrit Journal for Political Science
مجلة تكريت للعلوم السياسية
IRAQI Academic Scientific Journals
https://iasj.rdd.edu.iq/journals/

No.42

الاستراتيجيات الدولية لمواجهة التهديدات السيبرانية وحماية الاقتصاد العالمي: دراسة حالة الصين وفرنسا

International Strategies for Countering Cyber Threats and Protecting the Global Economy: A Case Study of China and France

Dr. Ali Mahmood Salman [a]
Ministry of Higher Education and Scientific Research [a]

م.د. علي محمود سلمان * [a]
وزارة التعليم العالي والبحث العلمي \ الدائرة القانونية [a]

A r t i c l e i n f o.

Article history:
Received 12 Oct.2025
Received in revised form 10 Dec. 2026
Accepted 23. Feb. 2026
Final Proofreading 15 Mar. 2026
Available online: 31. Mar .2026

Keywords:
- Cybersecurity governance
- international strategies
- global political economy
- cyber threats
- global governance

Abstract: The problem of cybersecurity has become an urgent topic of international concern with national security, international relations and economic stability being the points of concern at the international level. With the aim of examining the development and execution of policies by governments to thwart cyber-attack and guard critical infrastructures, this research will provide a comparison between China and France. The analysis brings up some of the major dimensions of the governance such as: legal frameworks, risk management, safety culture, technology sovereignty, incident response and international cooperation among others. The results depict two unlike structures. The multi-level cooperative strategy of France combines national investment with European policies and transatlantic relationships whereas China follows the state-centric and sovereignty-oriented approach which prioritizes the regulation, technological independence, and centralized governance. The paper highlights essential differences in global alignment, openness and inclusiveness, and expounds how these strategies define international collaboration and national resilience. The paper adds to political science debates about governance of

*Corresponding Author: Ali Mahmood Salman, Email: ali.mahmood.s@mohesr.edu.iq, Tel: XXX, Affiliation: Ministry of Higher Education and Scientific Research \ Legal Department

cybersecurity by offering lessons in one of the cases in the form of a case study. It also gives policy implications on how models can be developed between the national sovereignty and enhancement of international security.

معلومات البحث:

تواريخ البحث:

الاستلام: 12 تشرين الثاني 2025

بعد التنقيح 10 كانون الأول 2026

القبول: 23 شباط 2026

التدقيق النهائي 15 اذار 2026

النشر المباشر: 31 اذار 2026

الكلمات المفتاحية:

- حوكمة الأمن السيبراني
- الاستراتيجيات الدولية
- الاقتصاد السياسي العالمي
- التهديدات السيبرانية
- الحوكمة العالمية

الخلاصة: أصبحت مشكلة الأمن السيبراني موضوعًا ملحًا على الصعيد الدولي، حيث تُعدّ قضايا الأمن القومي والعلاقات الدولية والاستقرار الاقتصادي من بين أهمّ القضايا التي تُثير القلق على المستوى الدولي. بهدف دراسة تطوير وتنفيذ السياسات الحكومية للتصدي للهجمات السيبرانية وحماية البنى التحتية الحيوية، تُقدّم هذه الدراسة مقارنة بين الصين وفرنسا. يُسلّط التحليل الضوء على بعض الأبعاد الرئيسية للحوكمة، مثل: الأطر القانونية، وإدارة المخاطر، وثقافة السلامة، والسيادة التكنولوجية، والاستجابة للحوادث، والتعاون الدولي، وغيرها. تُظهر النتائج هيكلين مختلفين. تجمع استراتيجية التعاون متعددة المستويات في فرنسا بين الاستثمار الوطني والسياسات الأوروبية والعلاقات عبر الأطلسي، بينما تتبع الصين نهجًا يتمحور حول الدولة ويركّز على السيادة، ويُعطي الأولوية للتنظيم والاستقلال التكنولوجي والحوكمة المركزية. تُبرز هذه الورقة البحثية اختلافات جوهرية في التوافق العالمي والانفتاح والشمول، وتُوضّح كيف تُحدّد هذه الاستراتيجيات التعاون الدولي والمرونة الوطنية. تُساهم هذه الورقة في النقاشات السياسية حول حوكمة الأمن السيبراني من خلال تقديم دروس مستفادة من إحدى الحالات في شكل دراسة حالة. كما تُقدّم آثارًا سياسية حول كيفية تطوير نماذج تُوازن بين السيادة الوطنية وتعزيز الأمن الدولي.

1. INTRODUCTION

Cybersecurity has become a defining challenge of the 21st century due to the rapid expansion of cyberspace, which has changed global politics and economics [1]. By 2021, almost 5 billion people were online, and the number is still rising, according to the International Telecommunication Union [2]. Connectivity has sparked innovation and expansion, but it has also created new opportunities for state-sponsored attacks, cybercrime, and threats to vital infrastructures like healthcare, finance, and energy [3]. Because vulnerabilities in one area can have repercussions on the global economy, states have an obligation to safeguard cyberspace that transcends national boundaries [4] [5].

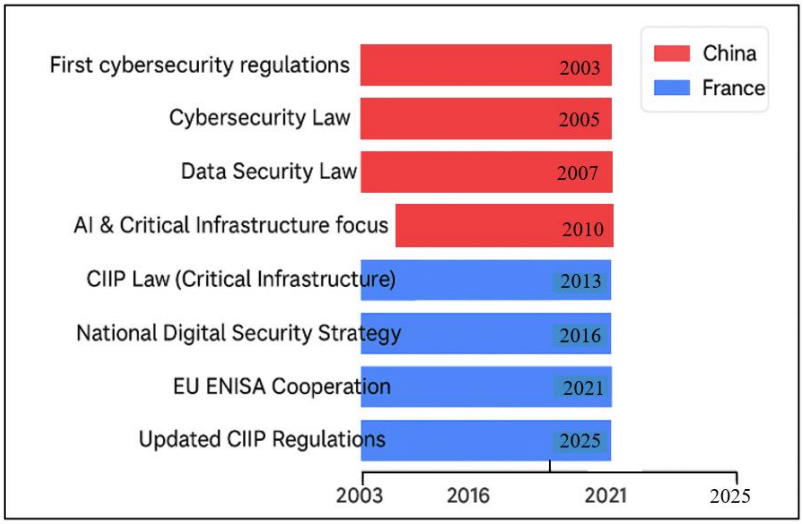


Figure 1: Milestones of the cybersecurity policy developments in China and France

Figure 1 compares a timeline of policies on cybersecurity in France and China. China began its work in 2003 by introducing the rudimentary regulations of cybersecurity, which was then supplemented by the official Cybersecurity Law in the same year, a Data Security Law in 2016, and a redirection towards critical infrastructure and AI in 2021. France, however, started with a Critical Information Infrastructure Protection (CIIP) Law in 2009, produced a National Digital Security Strategy in 2013, took part in cybersecurity collaboration in the whole EU through ENISA in 2015, and updated its CIIP regulations in 2017. The time timeline reflects the unique yet evolving positions on cybersecurity strategies embraced by both nations throughout the years (France with less emphasis on protection of critical infrastructure and more focus on European co-operation and China beginning earlier). National Cybersecurity Strategies have been prepared by other countries that have recognized this challenge [6]. The EU members have oriented towards regional harmonization according to the EU Cybersecurity act, UK has concentrated on resilience and partnerships with the private sector and the U.S has concentrated on deterrence and partnership with the private sector [7].

Meanwhile, cybersecurity has become a part of the general information security philosophy of Russia [8]. However, according to the variation in political ideologies, governmental systems and law, rival strategies have been developed which makes collaborating across the globe more challenging. France has integrated its cyberspace security plan in its geopolitical strategy at large [9]. Heightened antagonisms with China, especially over trade policies, human rights and technology power games have enhanced the determination by Paris to uphold critical infrastructure, technological autonomy and collaborate with EU and transatlantic allies [10]. Because China and France are two opposite but influential examples of international cybersecurity governance, this paper highlights the two nation-state case studies. Being an expansive online power, China is focusing on control, technological autonomy and centralized control in a state-centric, sovereignty-first approach [11]. France, on the other hand, is more of the European model of cooperation in that it maintains its national structures but relies on transatlantic alliances (NATO) and regional common organizations (ENISA, CERT-EU) [12]. By comparing these two

countries, one can obtain a unique point of view on the impacts of different philosophies of governance on the international economy protection against cyber threat.

The contributes of this study is as follows:

•To provide a comparative case study of China and France, two key powers, which have different cybersecurity philosophies.

•Suggesting a methodological framework to assess the national-level cybersecurity governance on the legal, institutional, and cooperative levels.

The identification of gaps and complementarities in national strategies that can be used to draw models of global cooperation can be highlighted.

•Providing policy suggestions to strike a balance between state sovereignty and collaboration in international governance of cybersecurity..

1.1 Research Gap

Although there is ample literature on national strategies related to cybersecurity, most comparative literature has been conducted on U.S. relations with the EU or between Western allies. Very little has been done to compare in detail how much more countries have resilience to global economies nudged by sovereignty or a Europe-type of countries nudged by cooperation. This paper fills this gap with a more systematic framework of pointing out, both, divergences and complementarities in their methods.

1.2 Hypotheses

H1: The Chinese approach to cybersecurity is more effective in regulatory control, and technology sovereignty than a French.

H2: The cybersecurity strategy of France has better international cooperation mechanisms than Chinese strategy.

H3: A hybrid approach between the regulatory model in China and the cooperative model in France may provide more balanced global approach.

1.3 Research Questions

1.What is the localization of cybersecurity in China and France in regard to its national strategies?

2.How are their strategies towards critical infrastructure similar and different?

3.What are the effectiveness of their strategies to protect the global economy against cyber threats?

4.What policy implications do these two models give?

2. Existing survey:

Dehnavi et al [13] analysed the role of strategic alignment between the United States and the United Kingdom in the Persian Gulf which put concentration on the military, political and security issues of the energy security. This paper will explore how coalition-based partnerships and policy ideas can be used to preserve stability and generate power in areas with few resources.

The paper explores these strategies and determines such advantages as enhanced deterrence, an enhanced presence in the region, and safe energy provisions. But it also notes challenges, including overcoming ideological differences and excessive dependence on specific alliances.

Pl этиа et al. [14] reviewed cybersecurity management of critical energy infrastructure, the United States, the United Kingdom, France, Estonia, and Lithuania, who also comment on national

strategies in the context of their extensive cybersecurity policies. It aims to assess the effectiveness of Critical Infrastructure Protection (CIP) measures and practical application of Global Cybersecurity Index (GCI). The analysis points to the role of adaptive strategies and mutual learning between countries, bringing out the benefits and drawbacks of various CIP models. However, the process of comprehensive implementation and alignment of diverse systems in nations becomes complicated.

Rotich et al. [15] examined how cyberterrorism was impacting the national security of Kenya and concentrated on the weaknesses caused by the rapid process of building ICT infrastructure. The research will seek to discuss the measures and controls undertaken to safeguard the critical cyber assets against ideological attacks involving personal information and financial resources. The paper shows that the rate of occurrence and magnitude of cyber threats in Kenya are upsurged owing to vulnerabilities in several sectors, which necessitate the need to enhance more defense mechanisms. Despite this, the evolving, ongoing, and complex nature of cyber threats presents ongoing challenges to put in place a comprehensive defense.

Were et al. [16] look at the application of UN Cyber Norms in Kenya to enhance harmony and security across the world with an emphasis on safeguarding essential infrastructure and responsible state conduct in cyberspace. The study aims not to reduce cyber threats but also to determine whether the adherence to norms helps increase the predictability, stability, and trust of states. Although knowledge, compliance and regulation are still absent, the conclusion is that by following the Nor, the cooperation between nations becomes better, the critical infrastructure is secured, and the national security is strengthened. Issues such as the transformation of norms into the binding agreement, the need to find equilibrium between the principle of non-intervention and self-defense, and building adequate capabilities in cyberspace governance at both the state and the corporate level can be among these challenges.

Al-Kasassbeh and Ghazleh [17] touch upon global and national attempts to defend against cybersecurity and the unguardedness unleashed by the use of technology and connectivity on a global scale. In addition to emphasizing the importance of international cooperation in the fight against international cybercrime, the research will demonstrate the ways in which cyberattacks pose threats to political, social and economic systems. The study concludes that due to the escalating risks that come with the increased technologically related financial and economic services, nations like Jordan are enhancing their legal and cybersecurity regimes. Although the creation of coordinated international responses and national abilities to withstand the emergence of new cyber threats have proven to be challenging, laws and national cybersecurity are being reinforced..

The results mention the need to develop global collaboration, effective intercountry partnerships, and effective protection of vital infrastructure to achieve cybersecurity and energy security. The quick ICT development and the low defence levels make the developing states susceptible compared to the developed ones, which focus on the coordination and resilience. Capacity-building, implementing flexible legislation, and inclusive partnership between the state and non-state are all required in the end to enhance stability in the long term.

3. Research Design

The current research utilises a case study approach to examine national measures aimed at stemming against cyber threats and safeguarding the global economy, focusing on China and France. Case study research is a method that enables one to go into the depth of understanding the development of complicate and contextual specific governance systems and decision-making processes. The two nations were chosen due to them being the best examples of the two different models of cybersecurity governance China is a more state-centric and sovereignty-based approach, whereas France is a multi-level cooperative approach, which is incorporated into the system of European Union and the transatlantic perspective.Table 1: Case Selection Justification

Country	Political System	Cyber Strategy Orientation	Reason for Selection
China	Single-party, centralized state	Sovereignty-first, state-led, integration with industrial/economic policy	Illustrates an authoritarian, state-centric model of cyber governance
France	Liberal democracy, EU & NATO member	Multilateral, regulation-based, institutionalized defence	Represents a democratic, alliance-driven approach to cybersecurity

To explain the choice of China and France, Table 1 compares the models of cybersecurity in the two countries: centralized and sovereignty-oriented Chinese model of wealthier relations bridges security, technology, and economic policies, whereas democratic and alliance-based French model prefer to collaborate within the EU and NATO. This comparison gives the study a good comparative focus.

3.1 Data Collection

This study gathered data by analysing documents on the strategies of the official national cybersecurity in the form of documents, policy papers, the legislation and governmental reports, and secondary literature. Key sources include:

•China: National Cybersecurity Strategy, Cybersecurity Law, policy statements of technological sovereignty and protection of critical infrastructure.

France: National Cybersecurity Strategy, ANSSI reports, EU cybersecurity regulations (EU Cybersecurity Act) and policy paper on transatlantic cooperation.

This was supplemented by other information within international cybersecurity reports and scholarly sources emphasizing on global cyber governance and critical infrastructure protection.

3.2 Analytical Framework

This research project analyzes the national approaches of Achieving Cybersecurity in China and France in six major dimensions. It begins by examining how the systems of governance operate and how the system of governance as in France based on collaboration and working together at the multi-level when compared to that of China which concentrates on the state as the main management body. Next, the legal regulations of the two countries are reviewed and the way, in which they address the matter of content control, data regulation, and information security. The main goal of risk management and critical infrastructure protection assessments is to protect major systems (energy, finance, national defense, and services to the people). Also, the study takes into

account the concept of technical sovereignty and examines how France depends on partnerships with Europe as compared to how China hopes to achieve an autonomous digital economy. The framework considers skills in crisis management and incident response (e.g. emergency management and Computer Emergency Response Teams (CERTs)). It also examines international engagement; China, plays in a zero-sum, sovereignty-driven manner whereas France plays cooperative engagement multilaterally and via its EU partners. Franco-Chinese relations have influenced the Indo-Pacific strategy of France and demonstrated how cybersecurity is reflected in the overarching geopolitical issues, including the military presence, weapons trade, and the need that other countries follow a human rights agenda.. The design is depicted in Figure 2.

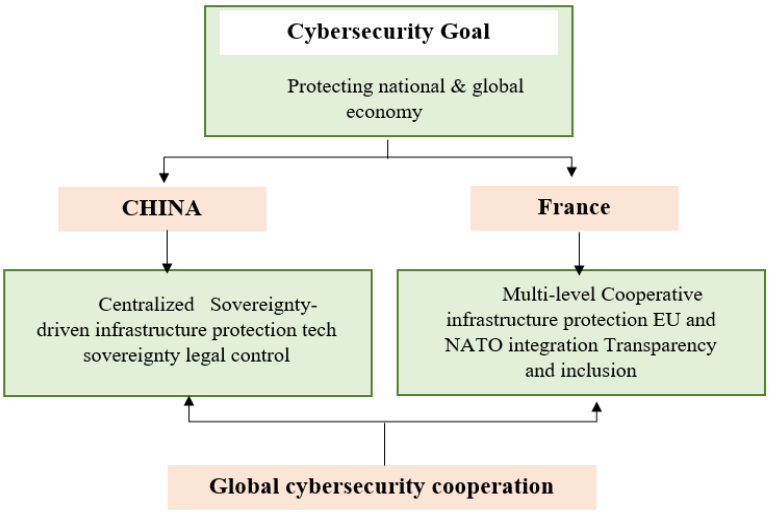


Figure 2: Cybersecurity Governance Framework

A 3.2.1. China. International strategies of cybersecurity.

Incident response and crisis management skills that are evaluated also include emergency planning and CERTs. Even though the Chinese approach is more sovereignty oriented, taking into account international collaboration is an indicator of multilateral and community oriented approach by France. The case of the Indo-Pacific strategy of France illustrates the connections between cybersecurity and more general geopolitical factors in the form of military force deployment into a nation, weapon sales, and human rights issues which are affected by hostility towards China. In the framework, cybersecurity is reflected (see figure 2). These frameworks emphasize two main goals: safeguarding critical information infrastructure (CII) and boosting the resilience of the digital economy. At institutional level, China has institutionalized its move by the Cyberspace Administration of China (CAC), which has the backing of the Ministry of Public Security and the Ministry of Industry and Information Technology. Under the Multi-Level Protection Scheme (MLPS 2.0) organizations have to designate their systems according to sensitivity and embrace security controls defined by state. In addition, the tendency towards Chinese technological autonomy, in which local innovations are created to track AI, 5G, and data security, evidences its long-term strategy of reducing its dependency on foreign technologies. The Chinese strategy can be assessed using the Cyber Security Management Model of Critical Infrastructure as the following:

•Legal Regulation → Strong. The Law of Cybersecurity is the binding guideline of data and CII protection and security.
•Risk Management → Centralized. The primary risk identification and mitigation are those that are conducted by government agencies and limit the independence of the private sector.
•Security Culture → Limited. The culture of organizations is based on compliance, and awareness is generated during the national campaign.
•Technology Management → Strong. Monitor local technologies and domestic research and development, as well as supply chain control.
-Opaque but advanced Incident Management. Rapid government actions, but low degrees of openness to external sources.
Chinas is a highly state-centric system, that is effective at regulation and technological control and ineffective at inclusiveness of governance, and building international trust.
In France, the concept of cybersecurity is defined as a collective responsibility of the state, the private operators, and the international partners. France has been committed in the long term by the 2015 National Digital Security Strategy and by instituting a regulatory framework of Critical Infrastructure Information Protection (CIIP) in 2013. The National Cybersecurity Agency of France (ANSSI) is also at the forefront of the implementation of these strategies in collaboration with the General Secretariat of National Defence and Security. France has chosen a two-pronged strategy of developing strong national structures and at the same time, involved itself in regional and international cooperation to a great extent. The cooperation with the European Union Agency on Cybersecurity (ENISA), CERT-EU and the NCIRC of NATO indicate that France engages in collective defence and resilience at European and transatlantic levels. France has also determined 12 crucial sectors and more than 200 operators of vital importance in the country, both of which are obliged to develop Operator Security Plans (OSP) and dedicated protection plans in partnership with ANSSI. Using the Cyber Security Management Model on Critical Infrastructure:
Legal Regulation → Strong. CIIP law and regulatory frameworks clearly outline responsibilities and designate operators of vital importance.
Risk Management → Moderate. Management of risks is operator-based and has certain shared rules, yet has no completely nationalized model.
Security Culture → Growing. There are training programs though the uptake of these programs by sectoral operators is uneven.
Technology Management → Moderate. France also invests in safe digital technologies, but partly leverages EU-level frameworks.
Incident Management → Functional. ANSSI leads on incidents, yet long-term resilience-based planning is still disjointed.
The multi-layered cooperative model adopted in France balances international alliance with national action, although it still struggles with creating a model at the national level that would bring about cohesion, consistency, and implementation among the operators.

Table 2. Analytical Dimensions of Comparison

Dimension	Key Indicators	China	France
Legal & Regulatory Frameworks	National cyber strategy, data laws, compliance structures	Cybersecurity Law, Data Security Law, state control of internet	National Cybersecurity Strategy, GDPR (EU-level), ANSSI regulations
Defence & Deterrence	Military doctrine, incident response, offensive capabilities	PLA Strategic Support Force, integrated cyber units	Military cyber command, ANSSI, participation in NATO Cyber Defence
Economic Measures	Supply chain protection, critical infrastructure, IP	Made in China, ICT self-reliance policies	EU-level resilience directives (NIS2), investment screening
International Engagement	Alliances, diplomacy, norms	Advocates "cyber sovereignty," participation in UN cyber groups	EU cyber diplomacy, NATO CCDCOE, Paris Call for Trust and Security in Cyberspace

The primary ideas for assessing and comparing China's and France's cybersecurity strategies are displayed in Table 2. Specific indicators were employed to operationalize each area: legal frameworks, defense and deterrence, economic measures, and international ways of participating. For example, France emphasizes EU-aligned regulations, public-private partnerships, and international collaboration, while China concerns substantially more over stringent state-based regulation and technological sovereignty. It is evident from this table how each dimension will be compared and assessed, ensuring a rigorous and transparent investigation.

3.3 Case Study Narratives

This part presents case study narratives comparing France and China and explaining their alternative approaches to cybersecurity governance. France pursues a multi-level, collaborative dimension (involving multiple actors) of governance, while China pursues a state-centric, sovereignty-focused set of standards. In both sections, the narratives reveal a greater political system, strategic objectives, and national involvement in international relations, respectively.

3.3.1. China: State-Centric, Sovereignty-Driven Approach

China places great value on a strong, centralized government and strict controls, and it considers cybersecurity a key aspect of national sovereignty. The state will monitor cyberspace to maintain political, economic, and social stability through content regulation, cross-border data flow regulation, oversight of infrastructure, etc. With significant protections in place to prevent attacks on critical infrastructure in key sectors such as energy, finance, transportation, defense, and public services, protecting critical infrastructure is paramount. At the same time, China is pursuing technical sovereignty by investing heavily in semiconductors, 5G, and AI technologies to reduce reliance on foreign technology and enhance resilience. Cybersecurity laws are enforced to deter cybercriminality, espionage, and other threats to information, using a mixture legal, administrative,

and technical measures for enforcement. Although China is engaged in global cybersecurity governance, its engagement is selective or strategic, focusing on alliances, coordinated projects, and bilateral engagement that meet China's national interests versus deep multilateral engagement. Mainly, China's approach includes strong states-driven systems, centralized form of decision-making, and attention to national sovereignty.

3.3.2. France: Multi-level Compromising.

France meets its transatlantic and European commitments in a multi-layer approach of cooperation, which links national efforts with regional and global frameworks. The multi-level governance ensures coherence, resilience and shared cybersecurity by the coordination between the national actors, European Union institutions (including ENISA) and NATO systems. The cybersecurity strategy adopted in France is, to a significant extent, based on the principles of public-private collaboration between the government players, the industry, and the civil society, which fosters a level of cyber security and response to cyber incidents. Similar to China, France is putting its national interests in securing critical infrastructure in the energy, financial, and defense sectors, but EU law and uniform security services provide a framework to support its proposals. The involvement of stakeholders, accountability to the people, and well-established data protection are a strong part of the GDPR, which is considered in alignment with the French regulatory paradigm of inclusiveness and transparency, as well. In addition, France is also engaged in the process of multilateral debates related to creation of international cyber principles and the joint strategies. Comprehensively, the approach taken by France is conducive to resilience and inclusion, is international governance standards-compliant, and, at the same time, balances it with national security and international cooperation..

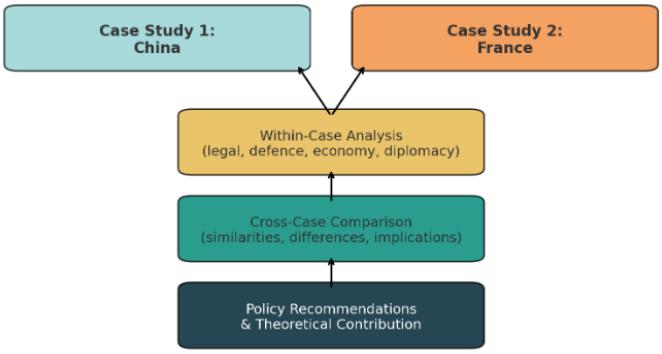


Figure 2: Comparative case study framework of China and France

Table 3: Key Aspects of Cybersecurity Strategies in National Security Frameworks (China vs France)

Cybersecurity Aspects	China	France
Cybersecurity framed as national sovereignty issue	✓	
Integration of cybersecurity with military strategy	✓	✓
Focus on technological sovereignty (5G, AI, chips)	✓	

Regional/International cooperation mechanisms		✓
EU/Transatlantic alignment		✓
Centralized governance and state control	✓	
Public–private partnerships in cybersecurity		✓
Protection of critical infrastructures (energy, finance, defense)	✓	✓
Strong legal regulations for cyberspace management	✓	✓
Cyber crisis response mechanisms (CERT/ANSSI/China CERT)	✓	✓
Emphasis on economic resilience against cyberattacks	✓	✓
Emphasis on transparency and inclusiveness in policy		✓
National data protection laws (e.g., Data Security Law / GDPR alignment)	✓	✓

4. Results and Discussion

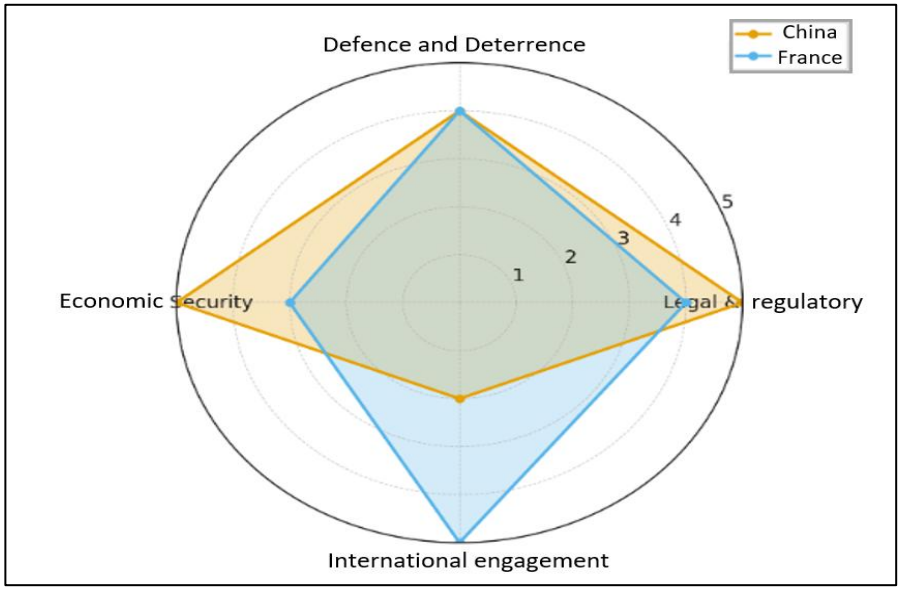
This section provides the comparative analysis of Chinese and French cybersecurity strategies and highlights the major strategic, legal and operational differences. The results show that underlying disparities in the governance systems and the legal frameworks as well as international interactions are a manifestation of the broader political and economic interests of each country.

Table 4: Comparative of China vs France in Cybersecurity Methodology

Dimension	China	France
Governance structure	Centralized, state-led	Multi-level, cooperative
Legal frameworks	Cybersecurity Law, strict content control	National law + EU Cybersecurity Act, GDPR alignment
Critical infrastructure protection	Strong government enforcement, comprehensive protection	National + EU-wide protection, public-private partnerships
Technological sovereignty	Emphasis on domestic innovation, 5G, AI, chips	Focus on interoperability, EU standard compliance
Incident response	China CERT, centralized reporting	ANSSI, EU-CERT, coordinated response
International engagement	Bilateral and selective partnerships	EU & NATO coordination, global governance forums
Transparency & inclusivity	Limited	High, inclusive stakeholder engagement
Economic resilience	Focused on national economic stability	Focused on EU-wide and global economic stability

Table 4 summarizes important China-France differences in cybersecurity methods along eight dimensions. The centralized, state-based system of governance directing China is favorable to its technologic-self-reliance within the country in many aspects and fields, including artificial intelligence (AI), 5G, and chip production, but also employs an authoritarian method of content control via its Cybersecurity Law. It has a centralized incident response system managed by China CERT in respect to incident response and a highly-regulated system of government-directed protection of critical infrastructure. In China, national economic stability is a primary factor, leading to bilateral or selective international relationships, as well as being open to low level of transparency or stakeholder participation. France, on the other hand, has implemented a multifaceted, collaborative governance framework that has complied with EU laws, such as the Cybersecurity Act and GDPR. It employs a coordinated response plan, including agencies like ANSSI and EU-CERT, and is based on public-private partnership to ensure infrastructure security. Moreover, France espouses high transparency, is more visible with regard to international fora and organizations like the EU and NATO, and works to make the EU and the world economically resilient.

Figure 3: Comparative Cyber strategy Dimensions (China Vs France)



The elements of France and China's cyber strategies are compared in Figure 3 in four key areas, consisting of economic security, legal and regulatory, international engagement, and defense and deterrence. China earns the highest score of five in both economic security and legal and regulatory. The countries receive similar scores in the defense and deterrence area. However, France earns a five in the area of international engagement, whereas China earns a two. This shows that China places greater importance on legislative frameworks and economic cybersecurity while France places greater focus on international engagement with cyber strategies.

Table 5: Implications of Cybersecurity Governance on the Global Economy

Dimension	Implications for Global Economy	Description
Attack Type	Threats to supply chain resilience	Supply chain and zero-day attacks disrupt global production and logistics
Critical Infrastructure	Impact on trade and essential service continuity	Compromise of critical infrastructure risks halting trade, transport, and energy
Regulatory Changes	Influence on financial stability and market confidence	Stricter laws and regulations affect cross-border investments and compliance
Sectoral Impact	Economic productivity and sectoral interdependence	Sector-specific disruptions affect global markets in manufacturing, healthcare, energy, etc.

Table 5 shows that economic impacts of cybersecurity governance and incidents in China and France relate globally. Attacks on the supply chain bring to the fore weaknesses in the infrastructure of international trade. The critical infrastructure (e.g., energy grid, transport networks) can be disrupted, which may jeopardize the provision of basic services and the vulnerability of the economy. Regulatory changes modify the compliance standards which impact on international business confidence in exchange of engaging in the financial markets. Sector impacts prove that interconnected industrial and service sectors can spread cyber risk via economies.

Table 6: Indicators of Cybersecurity Level in China and France

Country	Legal	Regulation	Good Governance	Risk Management	Security Culture	Technology Management	Incident Management
China	5	4	4	5	3	4	5
France	4	3	3	4	4	3	4

Table 6 highlights the cybersecurity capabilities of China compared to France along seven important constructs: framework/legislation, governance, risk management, security culture, technology management, and incident management. China has a more centralized disruption response strategy due to its higher overall rankings, and particularly in the constructs of legal, risk, and incident management. France is well positioned in security governance and security culture around matters of cooperation and public-private partnership. These differences illustrate how each country has a unique cybersecurity posture that supports their strategic objectives, and their ability to safeguard their economy against cyber-attacks.

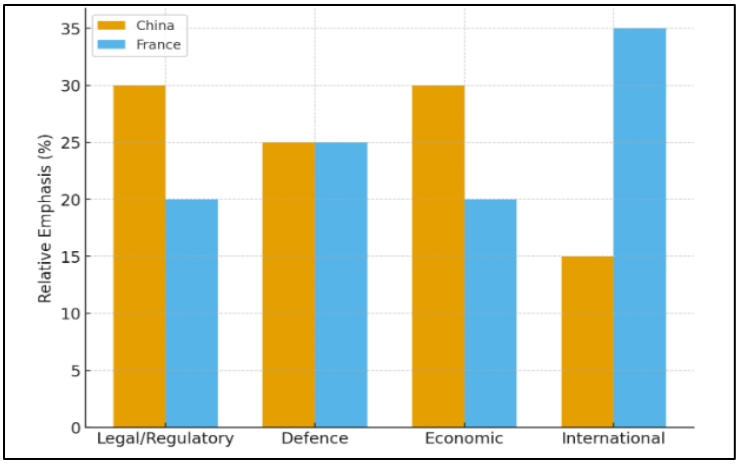


Figure 4: Emphasis on strategic Dimensions in policy Documents

Figure 4 shows the comparison in terms of the relative emphasis on four strategic dimensions in the policy documents of France and China. China puts more emphasis on legal/regulatory and economic factors, meaning that it focuses on home control and economic leverage, whereas France focuses the most on international participation and it is cooperative/ multilateral. The similarity of the importance of defense in the two countries is an indicator of the importance that military issues have to the two countries in terms of their strategies..

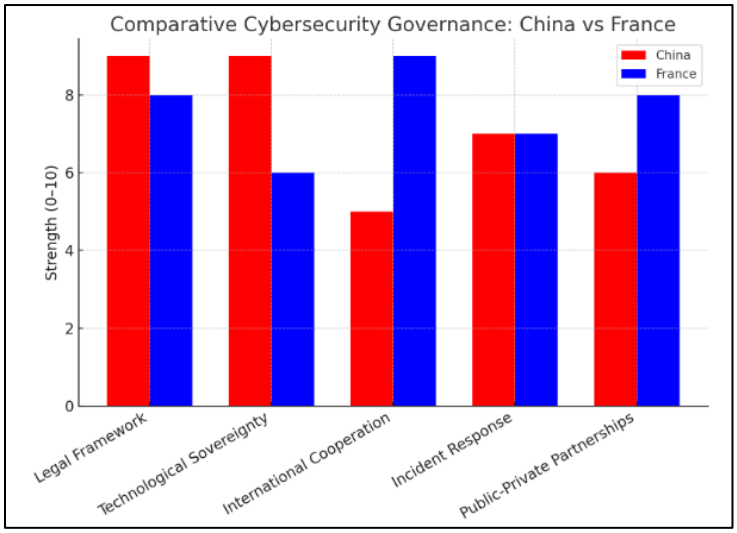


Figure 5: Comparative Analysis of Cybersecurity Governance Strength in China and France

In Figure 5, the bar chart presents a comparison of the cybersecurity governance strength in China and France in five categories. France is better than China in the domains of international cooperation and public-private partnership, but China has a higher score in technological sovereignty and legal framework, and both countries have the same score in terms of incident response. This is shown by different country priorities and cybersecurity governance and cooperation strategies.

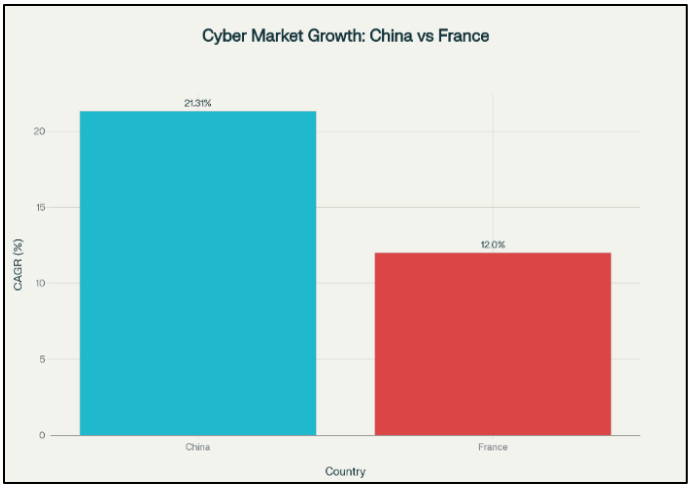


Figure 6: Cyber security growth in China Vs France

The expected cybersecurity market growth rates (CAGR%) for France and China from 2025 to 2033 are shown in Figure 6, underscoring the substantial disparity in each nation's aspirations for market expansion. The market in France is expected to increase at a rate of more than 12% per year, while the market in China is expected to grow at a CAGR of 21.31%.

Table 7: Comparative Trends in Cybersecurity Governance Between China and France

Dimension	Key Trend (China)	Key Trend (France)
Attack Type	Supply chain, AI, zero-day exploits	Ransomware, zero-day exploits
Critical Infrastructure	Comprehensive enforcement	Public-private partnerships
Regulatory Changes	Stricter law, higher penalties	NIS2 expansion, Campus Cyber
Sectoral Impact	Manufacturing, tech, logistics	Healthcare, energy, transport

Table 7 analyzes the prioritization of cybersecurity by type of attack, infrastructure, regulations, and sector, which reveal a difference in strategic approach between China and France. Both countries are rapidly adapting to emerging digital risk. France places greater importance to public-private collaboration and resilience by sector, particularly critical infrastructure such as electricity and healthcare, while China emphasizes regulation and innovation, and supply chain and high-tech industries. The evolving, adaptive development of national cybersecurity posture in response to an increasing range of global cyber threats.

5. Discussion

As the results section indicates, China and France are very acute in the approaches to cybersecurity, which mirror the differences in political, economic and strategic objectives. The state dominated, centralized system of governance of China is geared towards offering security to the major infrastructure of a highly controlled government and low foreign intrusion, hence, seriously concentrating on regulations and national technological autonomy. In contrast, France implements a multi-level cooperative governance model, which is highly coordinated with EU laws, is open in nature, has diversity of approach and broad public-private association to assist defence of critical infrastructure. In France, particularly, the culture of governance and concentration on collaborative structures is most appropriate, as well as security. China has well developed legal, risk

management and incident response response capabilities in the form of the centralized model and enforcement of regulations. China is more interested in the economic stability of its state economy and France is more interested in the greater stability of the EU and the wider economy. These differences make a significant difference in what a country can do to "respond" to an event, develop international collaborative arrangements and strategy, and where to prioritize their resources with respect to economic security. The comparative data are well presented to contain the strategic and economic implications. Speaking of the fact that China is geared towards high-technology levels and supply chain resilience, focusing on legal and regulatory frameworks and economic security, cybersecurity market can grow at a rapid pace (with a roughly 21.31 CAGR) as an emerging sector. On its side, France is interested in international involvement, which deregulates it in cross border cyber matters, and, via initiatives like Campus Cyber and NIS2, gives rise to a steady curve of growth (estimated at approximately 12% CAGR) as it markets the cybersecurity as a new industry. These changes of the types of attack, enforcement regimes and sectoral impacts are responses to the changing conditions of threat and are worth reflecting upon in the context of complementarity and synergies of the modes of cooperative multi-lateralism of France or sovereignty-based regulations of China. Such results suggest that national service versus global cooperation may be critical to uphold both domestic and international cyber and economic security in a globalized world.

6. Future Directions and Practical Implications

Although the work provides a broader perspective of cyber strategies by analysing China and France, the study also provides an opportunity to further research on other countries like the United States, India and Russia. Another possible area of future research is to go deeper into the scope of nations to include regional blocs like the EU, ASEAN and the AU as well as multilateral agreements under the UN, NATO or OECD to develop a further understanding of how group facilitation affects the economic stability of the world. Moreover, a swift development of technological solutions based on quantum computing and AI-based cyber protection to the cutting-edge 5G/6G networks, blockchain-based security mechanisms need a continuous investigation of the impacts of these alterations on governments, and international regulations of cyberspace. A longitudinal analysis of changes in the strategies of the response to the crisis over time and economic modeling can help policymakers and researchers build a clearer concept of the efficiency of various responses as necessary to anticipate the macroeconomic effects of cyber incidents on GDP, trade, and foreign investment.

This research has applications in a variety of fields. Policymakers can use comparative insights to help them harmonize cyber policies and create measures that foster confidence in order to minimize conflicts. To ensure that the disunity of cyber governance is lessened, international organizations can come up with optimum practices and strengthening of international cooperation structures. The results could be used by companies to streamline corporate cybersecurity to both domestic and global standards and improve supply chain, financial, and critical infrastructure security. The research also opens up new scholarly possibilities by encouraging an interdisciplinary research relating computer science, economics, and political science and

enhances the establishment of theoretical frameworks of resilience and cyber sovereignty. Lastly, civil society will be far more concerned about the impact of cyber policies on digital rights, privacy and confidence within the community, therefore, increasing the support of the approaches that will assist to find the balance between security and accessibility and openness.

7. Conclusion

Cybersecurity has not only become a gauge of international economic stability, but also a need of national security. The comparison of France and China illustrates how various risk management strategies, the central role of protection of critical infrastructure and participation in international relations are contextualized in relation to the living cooperative, multi-level approach to governance in France and the centralization based on sovereignty in China. Among these strategies are China is adopting good regulatory controls, legal requirements, technological autonomy which are helping to support the economical strength of the country and make the local cyber-security sector advance in a quicker manner. France as a member state of EU and NATO, has multi-lateral trust across borders and international stability through inclusive and open cooperation. The provided research proves that both of the frameworks do not imply the holistic approach to the changing reality of cyber threats. The cooperative model of France establishes a resilience relationship with partners, but can make decisions in times of crisis more difficult and longer, and the centralized model of China is efficient and controlling, although it may be less inclusive and less trusting towards international relationships. These cases are put together to show that a middle ground is reached on cyberspace between national sovereignty and international interdependence. The impact of such dynamics on the global economy is evident: in the context of cybersecurity rule, the interdependence of industries, market trust, holiness of supply chains, and security of critical infrastructure is established. The need of hybrid solutions regarding international cooperation and sovereignty, has proven in the case of internationalization problems in China and France; the future of avoiding problems of transnational cyberthreats will be pegged on our ability to incorporate technology innovation and institutionalize regulatory co-ordination and cooperation between national and multinational partners. This report, in its contribution to the existing debates on political science and international relations, points out the fact that cybersecurity measures are both technical reactions and incredibly political choices, and that by means of capitalising on the interactions of various governance modalities, national governments and international institutions will be able to build a more secure, resilient, and financially sustainable digital future.

REFERENCE:

1. Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. Journal of Financial Crime, 28(2), 359-374.
2. Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41(1), 5-32.
3. Afaq, S. A., Husain, M. S., Bello, A., & Sadia, H. (2023). A critical analysis of cyber threats and their global impact. In Computational intelligent security in wireless communications (pp. 201-220). CRC Press.
4. Verma, A., & Shri, C. (2025). Cyber security: A review of cyber-crimes, security challenges and measures to control. Vision, 29(4), 478-492.
5. Chatinakrob, T. (2024). Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty. Chinese Journal of International Law, 23(1), 25-72.
6. Kostyuk, N. (2014). International and domestic challenges to comprehensive national cybersecurity: A case study of the Czech Republic. Journal of Strategic Security, 7(1), 68-82.
7. Odebade, A. T., & Benkhelifa, E. (2023). A comparative study of national cyber security strategies of ten nations. arXiv preprint arXiv:2303.13938.
8. Calcara, A., & Marchetti, R. (2022). State-industry relations and cybersecurity governance in Europe. Review of International Political Economy, 29(4), 1237-1262.
9. WANJIRU, N. F., MALUKI, P., & SCIBORSKI, R. DIPLOMACY AND MITIGATION OF THE IMPACT OF GLOBALIZATION ON STATES SECURITY: A COMPARATIVE STUDY OF KENYA AND FRANCE. AJIS, 85.
10. AZUBUIKE, C. F. (2023). Cyber security and international conflicts: An analysis of state-sponsored cyber-attacks. Nnamdi Azikiwe Journal of Political Science, 8(3), 101-114.
11. Broeders, D., Cristiano, F., & Weggemans, D. (2023). Too close for comfort: cyber terrorism and information security across national policies and international diplomacy. Studies in conflict & terrorism, 46(12), 2426-2453.
12. Claudiu-Cosmin, R. A. D. U. (2024). THE PEOPLE'S REPUBLIC OF CHINA AND THE THREATS TO NATO'S CYBER SECURITY. Romanian Military Thinking, (4), 256-277.
13. Dehnavi, E. A., & Fiedler, R. (2025). The Alignment of the United States of America and the United Kingdom in Energy Security Strategy: A Case Study in the Persian Gulf.
14. Tvaronavičienė, M., Plėta, T., Della Casa, S., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. Insights into regional development, 2(4), 802-813.
15. Rotich, E. K. (2020). Cyber Terrorism and National Security in Africa: A Case Study of Kenya (Doctoral dissertation, university of Nairobi).
16. Were, T. O. (2021). Implementation of UN Cyber Norms in the Promotion of International Security: a Case Study of Kenya (Doctoral dissertation, University of Nairobi).
17. Al-Kasassbeh, F. Y., & Ghazleh, A. M. A. (2023). International and National Efforts to Protect Cyber Security: Jordan Case Study. International Journal of Cyber Criminology, 17(2), 350-363.