# International Cybersecurity Environmental Scan Template For China

Posted on December 4, 2023

Country: China

An international cybersecurity environmental scan should distinguish evidence from national stereotypes. China is a major digital power with an enormous domestic technology sector, extensive state regulation, growing cybersecurity capability, and a strategic interest in data, critical infrastructure, artificial intelligence, telecommunications, and military modernization. U.S. and allied agencies have attributed significant cyber-espionage and critical-infrastructure campaigns to actors linked with the People's Republic of China. Chinese authorities reject many foreign accusations and emphasize sovereignty, security, domestic law, and opposition to cybercrime. The resulting environment is defined by strategic competition, incompatible governance models, commercial interdependence, disputed attribution, and the risk that defensive measures may be interpreted as hostile preparation. The original template's questions remain useful, but claims that China is naturally aggressive or inevitably destined for "world dominance" should be replaced by a balanced assessment of laws, incentives, capabilities, vulnerabilities, and policy choices. (National People's Congress of the People's Republic of China, 2021)

## What Cultural and Institutional Characteristics Make Cyberspace Issues More Challenging?

Cybersecurity difficulties in China arise less from a single national personality than from the interaction of political institutions, economic scale, technology policy, and strategic doctrine. The Chinese party-state places strong emphasis on sovereignty, social stability, centralized political authority, and control of information. Cyberspace is therefore treated not only as a commercial or technical domain but as an arena of national security, ideological governance, and social management. This differs from models that prioritize decentralized private governance and broad freedom of expression, although Western governments also regulate security, data, and platform conduct.

China's scale adds complexity. It has a very large population of internet users, major cloud and telecommunications providers, globally important hardware and software supply chains, and enormous volumes of personal, industrial, and government data. Cyber rules therefore affect domestic companies, multinational firms, universities, infrastructure operators, and foreign governments. Language, regulatory opacity, overlapping authorities, and restrictions on cross-border data flows can make compliance and cooperation difficult. At the same time, describing China simply

as a “hub for hackers” erases legitimate Chinese businesses, researchers, users, and victims of cybercrime.

## State Security and Cyber Sovereignty

Chinese policy frequently uses the concept of cyber sovereignty: each state has authority to regulate networks, content, data, and infrastructure within its territory. This principle supports laws concerning cybersecurity, personal information, data classification, critical information infrastructure, national-security review, and cross-border transfer. Supporters argue that strong authority protects security and citizens from crime. Critics argue that broad security powers can enable surveillance, censorship, political control, and unpredictable obligations for organizations. For international relations, the challenge is that states disagree about where legitimate domestic regulation ends and harmful extraterritorial control begins.

## What Does the Current Chinese Cyber-Law Framework Include?

China’s framework includes the Cybersecurity Law, Data Security Law, Personal Information Protection Law, regulations concerning critical information infrastructure, and network-data security rules. The Data Security Law establishes classified and hierarchical management, obligations for processors, and protections related to important data and national interests. The Personal Information Protection Law requires lawful processing, responsibility, security measures, and conditions for cross-border transfers. The system contains concepts similar to international privacy and security regimes—such as consent, necessity, accountability, breach prevention, and sensitive information—but applies them within a stronger national-security and state-supervision framework. (Supreme People’s Procuratorate of the People’s Republic of China, 2021)

Organizations operating in China must understand data localization, security assessments, standard contracts, consent, important-data classification, and sector-specific obligations. Compliance cannot be reduced to installing antivirus software. It requires legal governance, data inventories, vendor management, access control, retention limits, incident response, and engagement with regulators.

## What Makes Cyber Attribution Difficult?

Cyber operations are designed to conceal origin. Attackers can route activity through compromised devices, use publicly available tools, impersonate other groups, purchase infrastructure, and exploit vulnerabilities before they are widely known. Attribution therefore combines technical indicators, infrastructure history, intelligence, victim patterns, operational timing, and strategic assessment. Public agencies may have classified evidence they cannot disclose fully. China’s denials and foreign

accusations must be evaluated through the quality of evidence rather than assumed true or false because of nationality.

Misattribution can escalate diplomatic conflict, while failure to attribute may allow repeated operations without consequence. Governments should use confidence levels, share indicators where possible, distinguish criminal groups from state-directed actors, and avoid presenting every incident involving Chinese-language tools as proof of state responsibility.

## What Major Threats Are Associated With PRC-Linked Actors?

U.S. and partner agencies have reported campaigns attributed to PRC state-sponsored actors targeting telecommunications, government, transportation, military, and other infrastructure networks. Recent advisories describe long-term access, exploitation of routers and edge devices, credential theft, living-off-the-land techniques, and global espionage. The strategic concern is not limited to theft of documents. Persistent access to critical systems could support intelligence collection, influence, or disruption during a future crisis. (Cybersecurity and Infrastructure Security Agency, 2025)

China is also a target of cybercrime, fraud, ransomware, intellectual-property theft, and foreign intelligence operations. A complete scan should assess two directions of risk: threats attributed to Chinese actors and vulnerabilities affecting Chinese organizations and citizens. Treating one country only as an attacker prevents meaningful cooperation on shared criminal threats.

## What Is Likely to Change Over the Next Decade?

Several developments are more plausible than a simple prediction of Chinese “cyber dominance.” First, artificial intelligence will increase automation in software development, vulnerability discovery, phishing, surveillance, malware analysis, and defensive monitoring. Second, competition over advanced semiconductors, cloud infrastructure, quantum technologies, undersea cables, satellites, and telecommunications standards will intensify. Third, China is likely to continue strengthening domestic technology supply chains and reducing dependence on foreign components where national-security leaders perceive vulnerability.

Fourth, cross-border data governance will become more complex as companies balance Chinese requirements with privacy, sanctions, export controls, and disclosure demands in other jurisdictions. Fifth, critical-infrastructure preparation will receive more attention because governments increasingly view cyber access as part of wider military deterrence. Finally, criminal ecosystems will adapt rapidly to digital payments, synthetic media, and AI-assisted fraud. No state is likely to achieve permanent control of cyberspace because the domain changes continuously and depends on international

networks and private technology.

## What Could Catalyze Change?

A major cyber incident affecting electricity, telecommunications, finance, healthcare, transportation, or government could lead to stronger regulation and international crisis. Military tension concerning Taiwan or the South China Sea could increase cyber preparation and the risk of miscalculation. A breakthrough in quantum computing or cryptography could require large-scale replacement of security systems. Economic pressure, sanctions, export controls, or supply-chain disruptions could accelerate technological separation.

Positive catalysts are also possible. A serious transnational ransomware event, financial fraud network, or vulnerability affecting multiple countries could create practical cooperation. Shared standards for reporting vulnerabilities, protecting civilian infrastructure, and responding to cybercrime may develop even when strategic rivalry continues. Change is therefore not driven only by attack; it can also arise from commercial need, diplomatic negotiation, public pressure, and technological interdependence.

## Could China Adopt a Different Economic Approach to Cyberspace?

China’s economic and security policies are already intertwined. Digital platforms, cloud services, e-commerce, telecommunications, manufacturing, and AI support growth, but policymakers also require data control, domestic resilience, and political oversight. A different approach could involve clearer cross-border data procedures, more predictable compliance, stronger privacy enforcement, and selective openness that supports investment. Conversely, rising geopolitical tension could produce tighter localization, security review, export controls, and technological separation.

Cyber defense is expensive, but China will not become “less reliant” on economic conditions. Security capability depends on research funding, workforce skills, semiconductors, software, infrastructure, and stable institutions. Excessive restrictions can reduce innovation and foreign investment, while insufficient protection can expose intellectual property and critical services. The policy problem is a trade-off rather than a shift from economics to pure aggression.

## Does China Do Enough to Address Cybercrime?

China has enacted laws, conducts domestic enforcement, participates in some international mechanisms, and publicly opposes cybercrime and terrorism. It has strong technical and regulatory capacity in many areas. However, external observers question transparency, due process,

consistency, cross-border cooperation, and whether state priorities distinguish politically sensitive activity from ordinary criminal enforcement. Cybercrime groups can also operate across jurisdictions, use encrypted communications, recruit money mules, and exploit countries where evidence-sharing is slow.

The answer is therefore neither a simple yes nor no. China has substantial laws and enforcement power, but effective cybercrime control should be judged through measurable outcomes: reported cases, prosecutions, victim assistance, international evidence exchange, disruption of infrastructure, protection of personal information, and safeguards against abuse. Voluntary information sharing is useful only when organizations trust that reporting will not create disproportionate legal or commercial harm.

## How Should Cyberterrorism Be Addressed?

Governments have legitimate reasons to prevent online recruitment, operational planning, financing, and threats connected with terrorism. The term should be defined narrowly. Broadly labeling dissent, journalism, or ordinary cybersecurity research as terrorism undermines rights and cooperation. Effective policy combines intelligence, lawful investigation, financial tracing, platform processes, community prevention, and judicial oversight. Removal of violent content may reduce distribution, but automated systems can make mistakes and extremist networks may migrate to smaller platforms. International cooperation should focus on conduct linked to violence while preserving lawful expression.

## What Recommendations Should a U.S. Ambassador Make?

A U.S. ambassador should not attempt to prescribe China’s domestic internet identity system or introduce technology unilaterally. The role is diplomatic: reduce risk, communicate concerns, protect citizens and businesses, support cooperation, and clarify consequences. Recommendations should begin with sustained cyber dialogue that includes crisis communication, norms concerning civilian critical infrastructure, and procedures for raising incidents before they escalate. Both countries should maintain points of contact capable of operating during political tension.

The ambassador should also support law-enforcement cooperation on clearly criminal activity such as child exploitation, financial fraud, ransomware laundering, and theft affecting ordinary citizens, provided evidence and human-rights safeguards are adequate. Technical exchanges can address vulnerability disclosure, secure routing, incident response, and supply-chain standards. Diplomatic engagement should be specific: broad accusations without evidence are less useful than presenting indicators, affected systems, requested action, and a timetable.

# Identity, Authentication, and Zero-Trust Security

The original recommendation concerning identification and authentication is relevant but poorly framed. Strong identity management does not mean giving governments unlimited access to every user. Organizations should use phishing-resistant multifactor authentication, least privilege, device verification, segmentation, privileged-access management, logging, and rapid revocation. Zero-trust architecture assumes that no user or device should receive permanent trust merely because it is inside a network. Privacy protections, necessity, proportionality, and oversight must accompany identity systems. Centralized identity data can become a powerful target if poorly protected.

# Artificial Intelligence: Benefit and Risk

AI can help detect anomalies, classify malware, prioritize alerts, identify fraud, automate security testing, and assist analysts. It can also create convincing phishing, generate malicious code, support surveillance, and produce false alerts. The statement that AI should be implemented “in all sectors” is too broad. Adoption should begin with defined problems, quality data, human review, security testing, and accountability. Critical decisions should not be delegated blindly to opaque models. Organizations need controls against poisoned training data, model theft, prompt injection, privacy leakage, and manipulated outputs.

# Protecting Critical Infrastructure

Critical infrastructure operators should inventory internet-facing assets, patch known exploited vulnerabilities, replace unsupported edge devices, segment operational technology, protect administrator credentials, monitor unusual routing and authentication, maintain offline backups, and rehearse manual operations. Procurement should require secure development and vulnerability disclosure. Because recent advisories describe compromises of routers and trusted connections, organizations should not focus only on endpoint antivirus. Network architecture, device configuration, and identity are central.

# Public-Private Cooperation

Most digital infrastructure is built or operated by private organizations, while governments possess intelligence, diplomatic authority, and law-enforcement powers. Cooperation requires legal clarity and two-way exchange. Companies should receive timely indicators and protection for responsible reporting; governments should receive enough information to identify campaigns. Agreements should define confidentiality, use of data, and escalation. Joint exercises can test response across telecommunications, energy, finance, healthcare, and transportation.

# International Norms and Confidence-Building

The United States and China disagree on many norms, but limited agreements can still reduce harm. Possible areas include protecting emergency health services, avoiding attacks on nuclear safety systems, communicating major vulnerabilities, and cooperating against transnational financial crime. Confidence-building measures do not require trust in every domain. They create procedures for managing mistrust. Verification and consequences remain necessary because statements alone will not prevent covert operations.

# Potential Impact of the Recommendations

Improved dialogue and technical communication could reduce accidental escalation and shorten incident response. Stronger authentication and network segmentation would make espionage and disruption more difficult, though determined actors could adapt. AI governance could improve defensive efficiency without creating uncontrolled surveillance or automated errors. Law-enforcement cooperation could disrupt criminals who exploit gaps between jurisdictions. Public-private exercises could reveal dependencies before a crisis.

There are also risks. Information sharing may expose sensitive sources, be used for political control, or create false confidence. Tighter technology restrictions can fragment the internet, increase costs, and reduce scientific exchange. Aggressive attribution and retaliation can escalate conflict if evidence is incomplete. The recommendations should therefore be implemented with oversight, proportionality, and measurable objectives.

# Conclusion

China’s cybersecurity environment is challenging because it combines vast digital scale, centralized political governance, strategic competition, sophisticated technology, restrictive data rules, and disputed cyber attribution. PRC-linked state actors are credibly associated by multiple governments with significant espionage and infrastructure campaigns, but that evidence does not justify describing all Chinese people or organizations as malicious. China also regulates cybercrime, protects data under its own legal framework, and faces threats. Over the next decade, AI, supply-chain competition, critical-infrastructure risk, and cross-border data rules will become more important. A productive U.S. strategy should combine strong defense and evidence-based attribution with crisis communication, narrow criminal cooperation, privacy-respecting identity security, responsible AI, and international norms. Cybersecurity cannot be solved through assumptions of inevitable dominance; it requires continuous risk management among deeply interconnected rivals.

# References

Cybersecurity and Infrastructure Security Agency. (2025). *Countering Chinese state-sponsored actors' compromise of networks worldwide to feed global espionage systems* (AA25-239A).

National People's Congress of the People's Republic of China. (2021). *Data Security Law of the People's Republic of China*.

Supreme People's Procuratorate of the People's Republic of China. (2021). *Personal Information Protection Law of the People's Republic of China*.

U.S. Department of Defense. (2025). *Military and security developments involving the People's Republic of China*.

U.S. Office of the Director of National Intelligence. (2026). *Annual threat assessment of the U.S. intelligence community*.