China Aerospace Studies Institute

Commander's Toolkit for China

PLA Cyber

Statement by the FBI

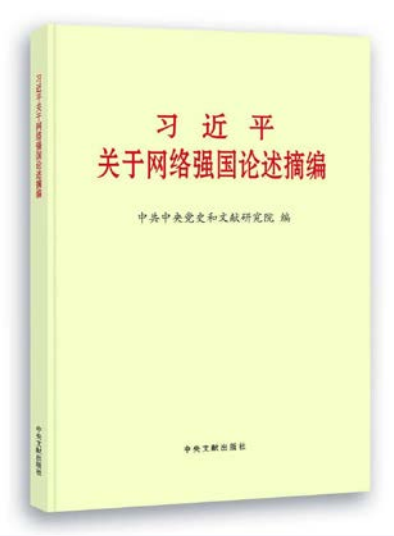
China is found to be the source of most cyber attacks on the US than all other nations combined.

Defense White Paper (2010)

- First mention of “cyber” in a strategic document
- *“China’s national defense is tasked to guard against and resist aggression, defend the security of China’s lands, inland waters, territorial waters and airspace, safeguard its maritime rights and interests, and maintain its **security interests** in space, electromagnetic space and **cyberspace**.”*
- *“**Some powers** have worked out strategies for outer space, cyber space and the polar regions, developed means for prompt global strikes, accelerated development of missile defense systems, enhanced cyber operations capabilities to occupy new strategic commanding heights.”*

“Cyber Superpower” Narrative

- First became prominent in early 2014 around the time of the first meeting of the new Central Leading Group for Cybersecurity and Informatization, headed by Xi Jinping (put himself at the center of cyber)
- unifying slogan around which a host of national and local policies on cyberspace and digital technology (was framed as a top-line strategic concept)
- XI: landmark April 19, 2016, **speech** to the Work Conference for Cybersecurity and Informatization and a **follow-up speech** two years later. It was even featured in a rousing patriotic song
- Drafters of the Cyberspace Administration of China“If our party cannot traverse the hurdle represented by the Internet,” “it cannot traverse the hurdle of remaining in power for the long term.”
- Cyberspace is the “the nerve center of both national governance and various spheres of society”



“Without cyber security, there would be no national security, and without informatization, there would be no modernization.”

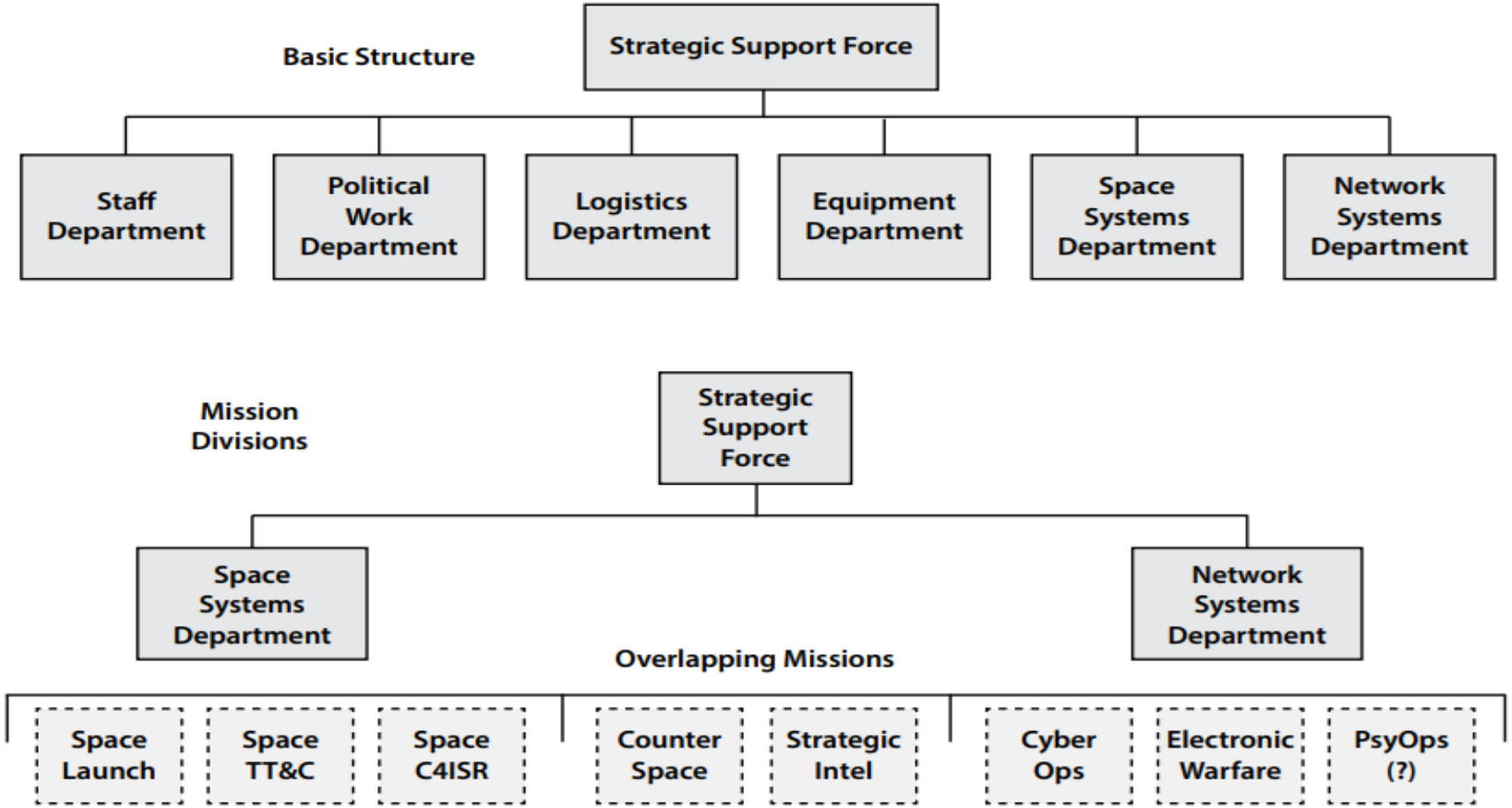
Military Strategy 2015

- Heavy emphasis on threat of attack
- *"Space and cyberspace have become n**ew commanding heights in strategic competition** among all parties. The form of war is accelerating its evolution to informationization."*
- *"Cyberspace has become a new pillar of economic and social development, and a new domain of national security. As international strategic competition in cyberspace has been turning increasingly fiercer, quite a few countries are developing their cyber military forces. Being one of the **major victim**s of hacker attacks, **China is confronted** with grave **security threats** to its cyber infrastructure. As cyberspace weighs more in military security, China will expedite the **development of a cyber force**, and enhance its capabilities of cyberspace situation awareness, **cyber defense**, support for the country's endeavors in cyberspace and participation in international cyber cooperation, so as to stem major cyber crises, ensure national network and information security, and **maintain national security and social stability.**"*
- After this document came wide ranging reform to the PLA…

People's Liberation Army Strategic Support Force (PLASSF)

- Established on 31 December 2015
- **Consolidated** China's space-, electronic-, cyber- and information-warfare capabilities
- Charged with securing the information domain while working closely with the other PLA services to execute regional and global military operations
- Like a functional combatant command of the U.S. armed forces, one that combines the activities of the National Geospatial-Intelligence Agency, the National Reconnaissance Office, Space Force, the National Security Agency, and U.S. Cyber Command
- Divided into 2 Departments
  - Space Systems
  - Networks Systems
- Arguably the single most well-funded and capable Chinese agency for carrying out **joint cyberspace operations** in peacetime or wartime

Figure 2. Overall Structure of the SSF



Key: PsyOps: psychological operations; TT&C: telemetry, tracking, and control.

Advanced Persistent Threats (APTs)

- **APTs** = type of operation in which the goal of the network intrusion is not only to gain access to a server or system, but also to retain ongoing access and engage in protracted cyber operations.
- Many APTs linked to PLA (as well as Ministry of State Security)
- Example: APT 1 (Unit 61398)
  - linked to a wide range of cyber operations targeting U.S. private sector entities for espionage purposes
  - systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously.
  - most commonly observed method of initial compromise is spear phishing.
- Example: APT 12
  - targets are consistent with larger People's Republic of China (PRC) goals. Intrusions and campaigns conducted by this group are in-line with PRC goals and self-interest in Taiwan.
  - utilize phishing as a malware delivery method
- **Full Mandiant APT List** https://www.mandiant.com/resources/apt-groups

National Cyberspace Security Strategy 2016
Opportunities

- Humankind's social historical development process
- New channels for the **dissemination of information**
- New spaces for **production** and life. (learning, life, work)
- New drivers for **economic development.** (upgrading of traditional industries, and new technologies, new business models)
- New carriers for **cultural flourishing** (enriched cultural / spiritual)
- New platforms for **social governance.** (e-government applications, citizen participation)
- New nodes for **interaction and cooperation** (global village, community of common destiny)
- New territories for **national sovereignt**y (equal importance to land, sea, air and space)

National Cyberspace Security Strategy 2016
Grave Challenges

- Cybersecurity situation is growing more severe every day
- Cyber penetrations harm **political security**. (social unrest)
- Cyber attacks threaten **economic security**
- Harmful online information corrodes **cultural security** (violate socialist core values)
- Online terrorism, law-breaking and crime are destroying **social security** (incite, plan, organize and carry out violent terrorist activities)
- **International competition** in cyberspace is rapidly unfolding. (norm-setting power, arms race in cyberspace)

National Cyberspace Security Strategy 2016
Objectives

- **Peace**: threat controlled, conflicts prevented
- **Security**: risks controlled, national systems perfected, core tech developed, talent to meet demand
- **Openness:** information technology standards, policies and markets
- **Openness:** Global cooperation -technology exchange, attack on cyber terrorism and cybercrime, “win-win”
- **Order**: public’s right to know, right to participate, right to express opinions, right of supervision and other such lawful rights and interests in cyberspace are to be fully protected

National Cyberspace Security Strategy 2016
Principles

- Respecting and protecting **sovereignty i**n cyberspace **(don't i**nterfere in the domestic affairs or engage in, connive in or support online activities endangering national security)
- **Peaceful use of cyberspace:** resist arms races in cyberspace, and prevent conflicts in cyberspace; mutual respect)
- Governing cyberspace according to the **law** (protect personal privacy, and protect intellectual property rights.)
- Comprehensively manage c**ybersecurity and development**.(quotes Xi: Without cybersecurity, there is no national security, and without informatization, there is no modernization.)

National Cyberspace Security Strategy 2016
Strategic Tasks

- Resolutely defending **sovereignty** in cyberspace.
- Resolutely safeguard **national security**.
- Protect **critical information infrastructure** (information infrastructure that affects national security, the national economy and the people's livelihood)
- Strengthening the construction of **online culture** (culture battlefield construction / Firmly attack the dissemination and spread of rumours)
- Attacking **cyber terrorism,** law-breaking and crime.
- Perfect **network governance** systems.(legal norms)
- Implement the **cybersecurity talent** project
- Enhancing **cyberspace protection c**apabilities. (forcefully develop cybersecurity defence means)
- Strengthening **international cooperation** in cyberspace. (international cyberspace dialogue and cooperation, and promote the reform of the global Internet governance system; UN; support poor countries infrastructure (BRI))

International Strategy of Cooperation on Cyberspace (2017)

- Strategic Goals
  - **Peace (**Safeguarding Sovereignty and Security)
  - Developing a System of **International Rules** (Norms)
  - Promoting a **Fair Internet Governance**
  - Protecting **Legitimate Rights** and Interests of its Citizens
  - Promoting **Cooperation** on Digital Economy
  - Building Platform for **Cyber Culture Exchange**
- Note **armed forces** play a key role in protecting China's sovereignty and other interests in cyberspace

Defense White Paper (2019): **China's National Defense in the New Era**

- Identifies **safeguarding** China's security interests in outer space, electromagnetic, space and **cyberspace** as some of the **fundamental goals** of China's national defence
- Actively participating i**nternationally** on rules and **norms** in cyberspace that are fair and equitable
- maintain national **cyber sovereignty**, information security and social stability.
- China's **armed forces** have 'accelerated the building of their **cyberspace capabilities** consistent with China's international standing and status
- Key functions of the **SSF** as supporting forces in the battlefield and providing information communications, information security and new technology across the PLA

Science of Military Strategy 2020

- Core textbook for senior PLA officers on how wars should be planned and conducted at the strategic level
- Over the last three decades, China's two premier defense institutes—the Academy of Military Sciences (AMS) and NDU—have produced several editions
- Chapter 22: Cyberspace Power Construction and Development
- 3 Parts: Trends, Capability Requirements, Measurements
- "Cyberspace has become a new space for military conflict, and cyberspace power, as a new combat force that adapts to the transformation of war patterns, has become an important part of the country's military power." (similar to 2013 version)

SMS 2020:
Power Construction and Development Trends

- **Towards a critical combat force** (3 stages)
  - 1. maintain uninterrupted, high-efficiency and high-quality network information interaction; C4ISRK
  - 2. deal w/ cybercrime and hacker attacks
  - 3. cyberspace operations: Prevent the enemy from controlling the network guarantees victory (lose the network lose the war)
- ***Development towards formalization and specialization***
  - *cyber warfare has shifted from the guerrillas to the regular army*
  - *knowledge-intensive and technology-intensive high-tech force*
- ***Development towards weaponization and actual combat***
  - weaponized computer software will continue to penetrate the Internet and military networks (USA best)
- ***Integration of military and civilian* (MCF)**
  - Just mil influence limited / civ advantage
  - Cyberspace operations are not divided into military and civilian use, technically, and tactically

SMS 2020:
Capability Requirements

- **Cyberspace Reconnaissance**
  - Carry out on enemy computer information systems to obtain intelligence information: network, electromagnetic, media
  - most common form of military conflict in cyberspace
- **Cyberspace Attack**
  - Offense > Defense
  - Paralyze, steal info, simulate false info (ex./ stuxnet)
- **Cyberspace Protection**
  - shield to guard the information frontier (more difficult)
  - intrusion detection, anti-virus, encrypt-data
- **Network Ops and Maintenance Recovery**
  - Determine timely and comprehensive perception of the battlefield situation of commanders at all levels; close cooperation and the ability to coordinate at a high degree of weapon platforms
  - Recovery critical to success

SMS 2020:
Measures for Construction & Development

- **Building an integrated command and mobilization system for reconnaissance, offense and defense in cyberspace**
  - maximize the formation of an overall joint force, rather than the ability to fight alone
- **Speed up the development of cyberspace resources**
  - electromagnetic spectrum resources (mil capabilities nav, com, radar, etc)
  - network information resources (US “big data”)
  - information system resources (Maximize the utilization of software and hardware resources)
- **Promote actual combat training of cyber warfare troops**
  - most important factor in exploring new combat styles and maintaining a high degree of war preparedness; combine strategic with technological innovation (US National Cyber Range - DARPA)
- **Establish and improve laws and regulations on the construction and use of cyberspace force**
  - US “Cyberspace Policy Evaluation-Ensuring Reliable and Robust Information and Communication Infrastructure”
- **Cultivate professional cyber warfare**
  - Train and possess a group of outstanding talents who are proficient in network warfare, “seize the commanding heights of network confrontation”
  - Strategist and Technical

Translated Strategy Documents

- **Defense White Paper (2010)** **http://english.www.gov.cn/archive/white_paper/2014/09/09/content_281474986284525.htm**
- **Military Strategy (2015)** http://english.chinamil.com.cn/view/2021-06/23/content_10053010.htm#:~:text=China%20will%20unswervingly%20follow%20the,never%20seek%20hegemony%20or%20expansion
- **National Cyberspace Security Strategy (2016)** https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/
- **International Strategy of Cooperation on Cyberspace (2017)** https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html#:~:text=The%20strategic%20goal%20of%20China's,peace%2C%20security%20and%20stability%20in
- **Defense White Paper (2019)** https://www.andrewerickson.com/2019/07/full-text-of-defense-white-paper-chinas-national-defense-in-the-new-era-english-chinese-versions/
- **Science of Military Strategy (2020)** **https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-26%202020%20Science%20of%20Military%20Strategy.pdf**

Teaching Notes PLA Cyber

- **Purpose:** Give students a better understanding of the PLA' s strategic mindset in cyberspace with the review of core documents (links included in slides and Appendix in this document)

SLIDES

- **SLIDE 2:** Statement by FBI
  - China has proven to be incredibly adept at offensive cyber campaigns. Here is a quick overview of threat: https://www.cisa.gov/uscert/china
  - Good to mention China calls US a hacking empire: https://www.youtube.com/watch?v=7pbb2NJbYzw
- *Note on Strategic Documents - at least skim through them, all links in appendix*
- **SLIDE 3:** Defense White Paper (2010)
  - Biggest thing here is simply to mention this is where CCP openly began discussing cyber in official strategic document
  - Establish Cyberspace as a security interest
  - **"Some powers"**
    - China is observing what their adversaries (like the US) are doing to address these"new strategic commanding heights" that come with the cyber domain
- **SLIDE 4:** "Cyber Superpower" Narrative
  - The biggest thing to understand here is cyber is not just a focus of just of certain departments in the CCP/ PLA but goes all the way to the top of leadership
  - Cyber is being pushed from the very top under Xi
  - Being strong in cyber is critical to China's "great rejuvenation" in Xi's mind
- **SLIDE 5:** Military Strategy 2015
  - Major document paving the groundwork for the PLASSF
  - Cyber has been named critical to national security and there needs to to be a force associated with it
- **SLIDE 6:** PLASSF
  - Review CASI's Primer chapter on PLASSF
- **SLIDE 7:** Structure of PLASSF
  - Simply emphasize the division of the Space and Network Systems department
  - Network Systems includes Cyber Ops as seen on chart
- **SLIDE 8:** APTS
  - Much of the specifics of PLASSF cyber ops are either classified or unknown
  - Mandiant has done a great job in open source - check out the link in the powerpoint
  - Picture: is the basic steps typically taken in APT from Define Target to Cover Tracks

- **SLIDE 9 -13:** National Cyberspace Security Strategy
    - Most current cybersecurity strategy from China
    - Note **sovereignty** as a key theme throughout this and remaining strategic documents. This is how China frames a lot of what they do in the cyber domain.
- **SLIDE 14:** International Strategy of Cooperation on Cyberspace (2017)
    - Note here and in other documents when they wrote about peace, fairness, etc what they mean is on the terms of the CCP
    - Cooperation is another. Cooperation = benefits the CCP.
- **SLIDE 15:** Defense White Paper (2019): China's National Defense in the New Era
    - Here they specifically mention SSF and its role in the cyber domain / PLA
- **SLIDE 16-19:** Science of Military Strategy 2020
    - Just to reiterate, SMS is a critical document to understanding the PLA's strategic mindset to include in the cyber domain (have a whole chapter)
    - Slide 17: The authors now almost universally use the phrase "**C4ISRK** system" rather than "C4ISR (command, control, communications, computer, intelligence, surveillance, reconnaissance) system", adding "kill (platforms)" to the mix. Most references to "C4ISRK" appear in the context of "networking systems", suggesting a growing need to also network weapon systems. This in turn should improve the PLA's ability to execute a notional "cross domain killchain".
    - Slide 18:
        - Note "Offense > Defense" - China is very capable coducting offensive cyber operations, but struggle to maintain their own networks security.
        - For your reference: Network secrets stealing is the use of security vulnerabilities in the enemy's network to enter the information system and reconnaissance C4ISRK system, electronic warfare system, and weapon control system. Electromagnetic theft is the use of various electronic reconnaissance equipment to search, locate, detect, identify, record and analyze the electromagnetic signals emitted (or radiated) by various electronic equipment in the enemy's computer information system, and decipher the information in the other party's computer information system. Relevant information and intelligence; media secrets refer to information obtained by obtaining information storage equipment through spies, hackers, and purchases from third parti**es.**
    - Slide 19
        - Actual Combat Training: Xi has emphasized the importance that training closely mimic that of real combat in a war. Previously the Red Team (PLA) de facto win in training exercises.
        - US Big Data / US National Cyber Range - DARPA) - China is studying what the US is doing in the cyber domain to help enhance their own abilities . They are alos studying US documents like US "Cyberspace Policy Evaluation-Ensuring Reliable and Robust

Information and Communication Infrastructure”

- **Cultivate professional cyber warfare**
  - You can mention the National Cyber Center (NCC)
  - China stated they have deficit of 1.4 million cybersecurity professionals (including needs in PLA)
  - Construction began in 2017 (still building) (four smaller cybersecurity parks and industrial bases in Chengdu, Shanghai, Shanxi, and Tianjin
  - will improve China’s cyber capabilities by focusing on two goals:
    - **cultivating talen**t
    - **spurring innovation**
  - Only “base” to merge government, industry, academia, research, and application of technology
  - 7 centers for research, talent cultivation, and entrepreneurship; two government-focused laboratories; and a National Cybersecurity School
  - Direct line to Cyberspace Affairs Commission
  - Address Weakness Areas
    - Talent
    - Innovation
    - Indidenous

APPENDIX

The CCP view the internet as a battlefield

- Chinese Communist Party leaders recognize that “the main battlefield for public opinion” is on the internet and must have a main force
  - “image sovereignty”
  - 2 million paid professional internet commentators (trolls)
  - CCP also draws on a network of more than 20 million part-time volunteers
  - “young cyber army” described as a “reserve force” capable of “resolutely resisting false statements and rumors, and fighting online public opinion wars.”
  - 120 “network civilian volunteers” for every 10,000 Chinese internet users.
  - Employed directly by Cyberspace Affairs Commissions (CAC) and Propaganda Departments nationwide
- Under Xi drastic shift in the CCP’s approach to governing cyberspace
  - deployment of these volunteers as a defensive measure against hostile foreign forces looking to smear the good name of China
  - Training: online public opinion management, press relations, and “credibility restoration”

OTHER IMPORTANT CYBER PLAYERS

1. Ministry of State Security

- Closest equivalent to CIA
- civilian intelligence, security and secret police agency of the People's Republic of China, responsible for counter-intelligence, foreign intelligence and political security
- Main organization responsible for influence-oriented cyber operations at home and abroad. It
- Become very adept at cyber attacks, work with criminal networks
- Advanced Persistent Threat (APT) 41 (Wicked Panda)
  - launched a “deliberate campaign targeting U.S. state governments” and has successfully attacked at least six state government networks by exploiting various vulnerabilities, including Log4j. (Mandiant)
  - most prolific and effective China-based adversaries from the mid 2010s into the 2020s. They have consistently expanded their target scope as well as their toolsuite while shifting from criminally focused operations to state-sponsored targeted intrusions (Crowdstrike)

2. Cyberspace Administration of China

- Established in 2013

- CAC was removed from State Council oversight and put directly under **Central Cyberspace Affairs Commision**
- dual state-party identity morphed away from just ensuring a clean, healthy, non-threatening internet to more broadly protecting **privacy and data security.**
- Responsibilities: in charge of **cyberspace security and internet content regulation**, major functions are directing, coordinating and supervising online content management and handling administrative approval of businesses related to online news reporting.
- Draft regulations that encompass online content, algorithms and cybersecurity issues
- **Data Security Law** and the **Personal Information Protection Law**
    - The PIPL contains provisions requiring all data processed by national agencies and so-called critical information infrastructure operators be stored in China. Entities that handle personal information reaching a certain threshold are also required to store user data within China. And the law requires companies to pass a security assessment organized by cybersecurity agencies, like the Cyberspace Administration of China, or to meet other compliance requirements, if they wish to transfer data abroad. Reinforces Beijing's ambition to defend its digital sovereignty. If foreign entities "engage in personal information handling activities that violate the personal information rights and interests of citizens of the People's Republic of China, or harm the national security or public interest of the People's Republic of China,"

LINKS TO STRATEGIC DOCUMENTS

Defense White Paper (2010)
http://english.www.gov.cn/archive/white_paper/2014/09/09/content_281474986284525.htm

Military Strategy (2015) http://english.chinamil.com.cn/view/2021-06/23/content_10053010.htm#:~:text=China%20will%20unswervingly%20follow%20the,never%20seek%20hegemony%20or%20expansion

National Cyberspace Security Strategy (2016)
https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

International Strategy of Cooperation on Cyberspace (2017)
https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html#:~:text=The%20strategic%20goal%20of%20China's,peace%2C%20security%20and%20stability%20in

Defense White Paper (2019) https://www.andrewerickson.com/2019/07/full-text-of-defense-white-paper-chinas-national-defense-in-the-new-era-english-chinese-versions/

Science of Military Strategy (2020)
https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-26%202020%20Science%20of%20Military%20Strategy.pdf