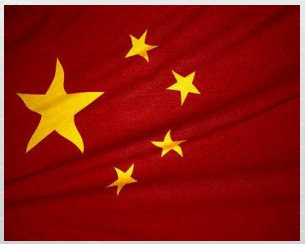
S. RAJARATNAM SCHOOL
OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University



Decoding China's CyberWarfare:
Perceptions, Strategies, and Capabilities

Dr. Michael Raska

Research Fellow
Institute of Defense and Strategic Studies
S. Rajaratnam School of International Studies

ismraska@ntu.edu.sg

Introduction:

- **Cybersecurity has become a major source of tension among many countries;**
  - rapid expansion and deepening technological sophistication of the Internet;
  - growing reliance of governments and societies on cyber-based systems
  - military operations, commercial activities, governance;

- **Western/U.S. intelligence assessments often point to a growing number of destructive cyber-attacks originating from China;**

- **Beijing has repeatedly denied carrying out cyber-attacks against any country, and called for both bilateral and multilateral cooperation to govern the Internet**

- **Cybersecurity is now a top priority in both Washington and Beijing;**
  - little progress in reducing suspicions and developing cooperation;
  - both U.S. and China are strengthening their capacity to engage in both defensive and offensive cyber operations;

→ **Important to examine Chinese views, beliefs, and assumptions on cybersecurity**

Outline:

Part 1. **Chinese viewpoints on four basic aspects:**

(1) Definition of Cybersecurity and Key Challenges;
(2) Cybersecurity Threats Posed by the U.S. and other countries;
(3) Origins and Motives Underlying These Threats;
(4) Chinese Preferences for Mitigating Cyber Threats;

Part 2. **Assessment of China's capability to conduct CNO**

(5) PLA CyberWarfare Strategy at the Campaign and Strategic Level;
(6) Principal Individual Actors & Entities;
(7) Cyberespionage

Conclusion: **The Future of Cyberwarfare**

Note on Sources:

Part 1. Chinese viewpoints on four basic aspects:

- Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations" (China Leadership Monitor, 2013);
- Jon Lindsay, “China and Cybersecurity: Political, Economic, and Strategic Dimensions” (IGCC, UC San Diego, 2012).
- The Information Office of the State Council, “The Internet in China” White Paper 2010.

Part 2. Assessment of China’s capability to conduct CNO

- The US-China Economic and Security Review Commission Reports;
- Mark Stokes and Russell Hsiao, “Countering Chinese Cyber Operations” (Project2029 Institute, 2012)
- Tobias Feakin, “Enter the Cyber Dragon: Understanding Chinese Intelligence Agencies’s Cyber Capabilities” (ASPI Special Report, 2013);
- Mandiant, “APT1 – Exposing One of China’s Cyber Espionage Units” (Mandiant Report 2013);

Part 1:

Chinese viewpoints on Cyber Security

Chinese Definitions of Cybersecurity:

To what extent and in what manner do Chinese definitions of cybersecurity and Chinese views on the cybersecurity differ from other countries?

1. **Authoritative Sources (PRC Government, if publicly available)**
2. **Quasi-Authoritative Sources**
3. **Non-Authoritative Sources**

- **Authoritative sources: do NOT provide detailed definition of cybersecurity and the challenges it poses:**

  - PRC government statements refer to the growth of the Internet;
  - The increasing dependence of many nations on cyber-based activities;
  - The potential dangers posed by cyber attacks or incursions;
  - The need for governments to provide more supervision over the Internet;

- **Non-Authoritative sources provide much more detailed discussion;**

→ **Apparent unanimity and support for official position / no internal debates**

General Perceptions:

Most Chinese view cybersecurity in similar terms as in other countries:

→ Protection of the Internet against harmful activities that undermine or affect China's national security, commercial, social, and individual interests;

"Cyber security is an international… issue and hacker attack is a common challenge facing the whole world."

"[The Internet is] transnational and anonymous; it involves multiple fields and multiple agencies, there is a coexistence of hardware and software, there is an overlap of the virtual world and reality."

Most Chinese have the same concerns as much of the rest of the world:

→ Harmful cyber-activities: efforts to crash, slow, or paralyze vital cyber-based infrastructure, diffusion of information or images harmful to the polity, society, or the economy, espionage, cyber crime, actions designed to weaken the capacity of the state to defend itself through military and other means.

Concept of "Cyber Sovereignty":

- Both Ministry of Foreign Affairs and Ministry of Defense officials often state that *"China is a major victim of hacker attacks."*

- Chinese military often cites statistics on the number of cyber-attacks on its systems, in large part to rebut foreign accusations that the PLA is conducting huge numbers of attacks on others;

- **Emphasis on cyber threats that challenge existing domestic social and political norms or values and sovereignty of the nation-state:**

Concepts: ***Sovereign "Virtual Territory" or "Cyber Sovereignty"***

→ The need for a government to identify the boundaries of such territory and protect it against cyber-based threats – Defend China's Cyber Sovereignty

→ Non-authoritative sources often cite the disruptive impact of social networking in the Middle East;

"Ideological Dimension":

Academy of Military Sciences (AMS): *"The strategic significance of the Internet lies in the fact that it has become an effective tool that beaks national boundaries, communicates information worldwide, and influences international and domestic affairs."*

→ **Acute sensitivity of the PRC government to potential threats posed by any "unregulated" activity → Strong Chinese concern with social disorder;**

→ **State-centric orientation toward cybersecurity** more than in Western democracies → **more direct, activist, and ideological role for government;**

"Freedom on the Internet is… subject to laws and morality"

→ **Many non-authoritative sources repeatedly assert that China is highly vulnerable to cyber attacks** because it relies primarily on developed countries (U.S.) fore core network technologies;

"Ideological" Dimension of Cybersecurity

Defense and expansion of "socialist ideology and culture";

“U.S. Dominance of Global Cyber System”:

Non-authoritative Sources:

U.S. dominance and de facto control over Internet technologies and cyber infrastructure:

- Source of instability and potential danger for the global cyber system;
- Many Chinese source declare that 10 (if not all) of the 13 so-called root servers essential to the function of the Internet are located in the U.S.;

“80% of the worldwide Internet data transmission and processing occurs in the U.S.”

Quasi-authoritative Sources are more direct:

“All root servers are under the unified control of the ICANN (Internet Corporation for Assigned Names and Numbers), which has the mandate of the U.S. government. It is responsible for the management of Internet root name servers, domain name systems, and IP addresses worldwide.”

“The Chinese Internet industry is running in the hands of the U.S.”

"U.S. Dominance of Global Cyber System":

Authoritative Sources:

Do not publicly identify the US government, much less Western governments in general, as the verifiable source of the major types of cybersecurity threats:

> *"As far as we know, cyber attacks against China mainly originate from the U.S. (as indicated by the apparent location of the attackers' IP address)… we are keenly aware of the complexity of the Internet environment so we do not come to the conclusion that it is the U.S. institutions or individuals that have carried out the attacks." [Foreign Ministry]*

Military Sources: *"As cyber attacks are transnational, anonymous and deceptive, often percolating IP addresses, we do not point fingers at the United States."*

PRC Defense Ministry officials, however, occasionally explicitly state that many attacks *"originated from the U.S."*

“U.S. Double Standard”:

Many Chinese sources regard Western and U.S. accusation that China engages in numerous cyber-activities against other countries as a sort of threat to China:

→ They consistently and vehemently deny such accusations as groundless, fraudulent, unsubstantiated, and hence unprofessional, while repeating the claim that *“China is opposed to all hacking and other forms of cyberattacks”;*

→ **At the same time, authoritative, quasi-authoritative, and non-authoritative Chinese sources also charge the U.S. pursuing a double standard** by accusing others of cyber-attacks, while conducting cyber-espionage itself (Snowden/PRISM)

Defense Ministry: *“Prism Gate reflects the real face and hypocritical deeds of a certain country.. This kind of double standard of taking advantage of advanced information technology to seek selfish gains on the one hand while making unfounded allegations against other countries is not conducive to peace and stability in cyberspace.”*

"U.S. Militarization of Cyberspace":

Non-authoritative sources more vocal:

By developing the means to conduct offensive cyberwarfare, the U.S. is militarizing cyberspace and prompting an international cyber arms race, thereby undermining efforts to increase cybersecurity and aggravating Sino-US relations:

"Certain countries are now speeding up the development of cyber war forces seeking military superiority in cyberspace, giving impetus to applying armed conflict methods in cyberspace, and drawing up cyber warfare rules in disguised fashion, with the result that the risk of military conflict in cyberspace is continuing to grow, posing an increasingly obvious threat to national security and international peace."

"The U.S. is trying to solely seize the hegemonic status in global cyberspace and also dominate the formulation of the rules of the game for cyber warfare through a series of strategic measures, thus capturing the commanding heights of future cyber warfare." [PLA Daily]

Chinese Preferences:

Authoritative Sources most often address the issue:
Foreign Ministry:

> *"China stands ready to work with the international community including the U.S. to carry out constructive dialogues and cooperation in the principles of mutual respect and trust so as to jointly safeguard peace, security, openness, and cooperation of the cyberspace."*

> *"The United Nations, we believe, is the most appropriate forum for deliberation and formulation of…international norms and rules on information and cyber-space security."*

→ **Code of Conduct of Responsible Countries for Cybersecurity (2011);**
→ **Foreign Ministry "Cyber Affairs Office" to coordinate diplomatic activities regarding cyber-affairs;**

→ **Bilateral working groups with key actors such as the U.S.**
(i.e. The annual China-U.S. Forum on the Internet Industry; Cyber Working Group under the framework of the S&ED")

Chinese Preferences:

Non-authoritative sources:

Emphasize the need to cooperate under the auspices of the UN to develop a common set of norms and regulations governing the Internet, PLUS:

→ The notion of "cyber sovereignty" should constitute a key principle guiding the establishment of common norms;

→ Such an international effort should oppose the militarization of cyberspace and ultimately end the allegedly unjust and threating pattern of U.S. dominance over the Internet;

→ Stronger PRC laws to govern the Internet, as part of the overall effort to develop a common approach in this area;

→ Chinese approach differs from the US, which believes that governments should take low profile in supervising and ordering the Internet, preferring instead a "multi-stakeholder approach";

Part 2:

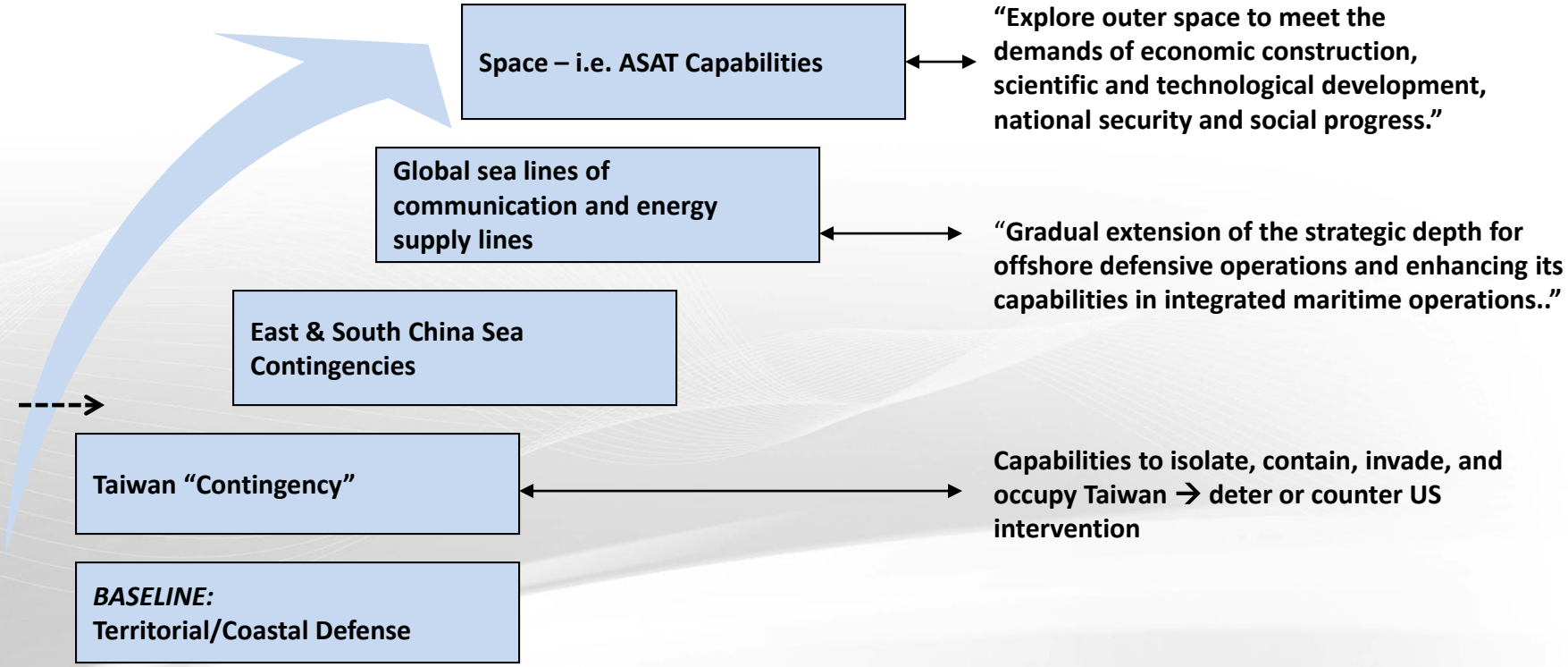
China's Cyber Strategies & Capabilities

PLA Strategic Priorities

"Limited, Local Wars under Informationnalized Conditions"

"Multilayered Active Defense"

"Diversified Missions"



Two-track vision of PLA's military modernization:

(1) Upgrading of existing equipment + selective introduction of new generation systems

(2) Transformation of the PLA

Integrated Network Electronic Warfare:
(wangdian yitizhan)

Coordinated use of CNO, electronic warfare (EW), and kinetic strikes designed to strike an enemy's networked information systems, creating "blind spots"

= Simultaneous application of electronic warfare and computer network operations against an adversary's C4ISR:

→ **EW and Counter-space Forces:** Attacks on vital targets such as an adversary's intelligence, surveillance, and reconnaissance (ISR) systems
- Electronic jamming, electronic deception and suppression to disrupt information acquisition and information transfer;

→ **CNA Attacks** on an adversary's data and networks will likely be the responsibility of **dedicated computer network attack and exploitation units;**
- Virus attacks, hacking to sabotage information processing;

Cyber Operations will be widely employed in the earliest phases of a conflict, and possibly preemptively against an enemy's information systems and C4ISR systems
→ the objective is to deny an enemy access to information essential for continued combat operations;

Information Dominance:

PLA assessments of current and future conflicts note that ***campaigns will be conducted in all domains simultaneously: ground, air, sea, and electromagnetic spectrum***

→ PLA's adoption of the "Informationized Conditions" doctrine:

Achieving information dominance is one of the key goals for the PLA at the strategic and campaign level, according to ***The Science of Military Strategy and The Science of Campaigns*** - two of the PLA's most authoritative public statements on its doctrine for military operations;

→ Seizing control of an adversary's information flow and establishing information dominance (*zhi xinxi quan*) are essential requirements in the PLA's campaign strategy and are considered so fundamental that *The Science of Military Strategy* considers them a prerequisite for seizing air and naval superiority;

→ Both identify enemy C4ISR and logistics systems networks as the highest priority for IW attacks, which may guide targeting decisions against the US or other technologically advanced opponents during a conflict

→ "blindness, deafness, or paralysis created by information attacks;

Space-Based Information Asset Control:

The PLA recognizes the importance of controlling space-based information assets as a means of achieving true information dominance, calling it the "new strategic high ground," and many of its advocates consider space warfare to be a subset of information warfare;

→ The PLA is seeking to develop the capability to use space for military operations while denying this same capability to an adversary;

→ PLA authors acknowledge that space dominance is also essential for operating joint campaigns and for maintaining the initiative on the battlefield;

→ Conversely, they view the denial of an adversary's space systems as an essential component of information warfare and a prerequisite for victory;

The PLA maintains a strong R&D focus on counter-space weapons and though many of the capabilities currently under development exceed purely cyber or EW options, they are nonetheless, still considered "information warfare" weapons;

PLA Information Warfare Planning:

Assessments of the likely impact on the adversary of a CNA strike on a given node or asset. These assessments, in turn, depend **upon detailed intelligence on the adversary's network, the C2 relationships;**

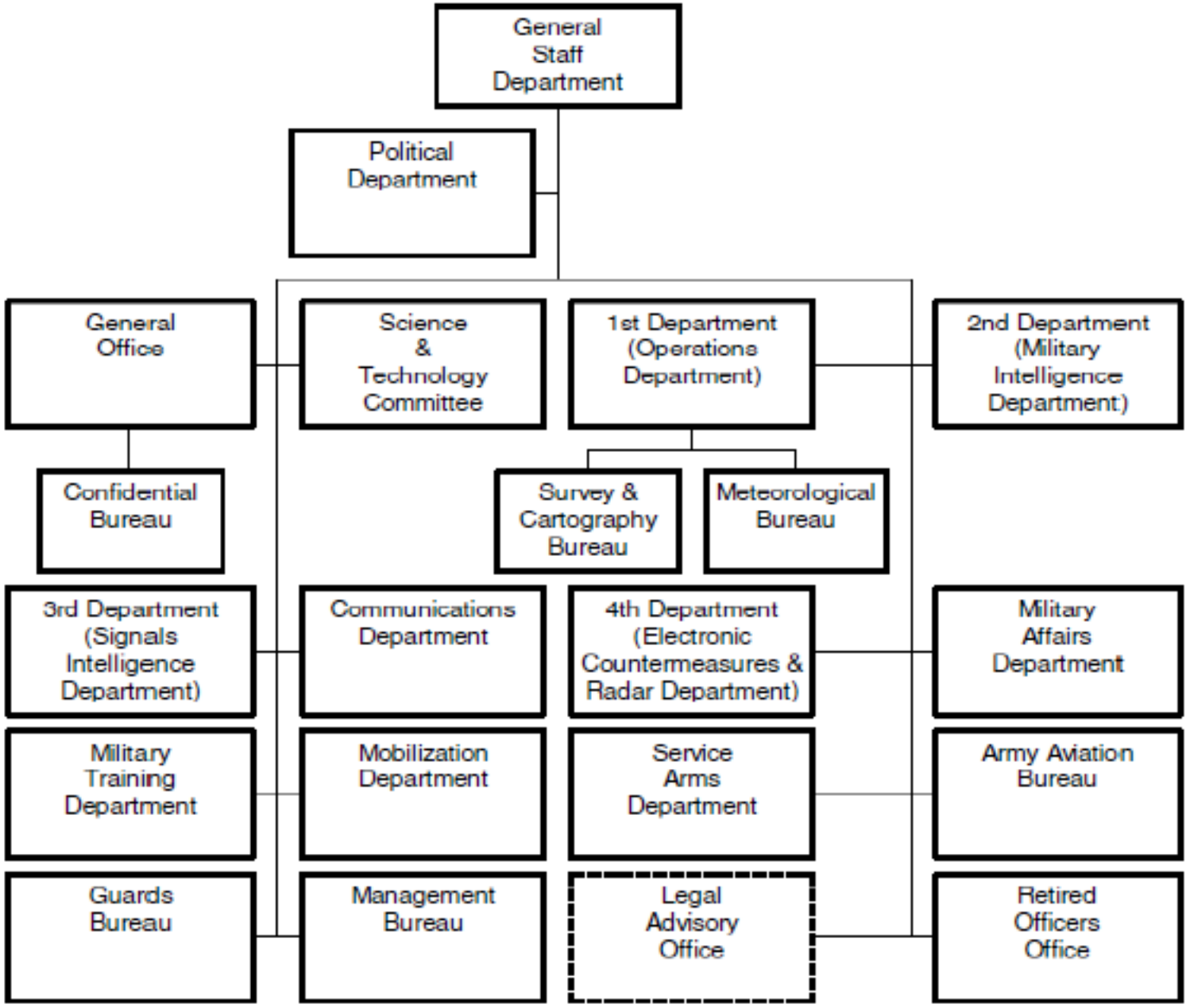
→ The *Science of Military Strategy* directs planners to ***"grasp the operational center of gravity and choose the targets and sequence for strike…"***

→ CNO or EW weapons employed by **tactical-sized units can strike strategic targets deep in the adversary's own territory** beyond the range of most conventional weapons, possibly changing the course of the conflict;

→ PLA IW planners note that **CNO is blurring the separation between the hierarchy of "strategy," "campaign," and "combat"** (or "tactics" in Western usage);

→ CNA planning also requires a ***nuanced understanding of the cultural or military sensitivities surrounding how a given attack*** will be perceived by an adversary;

Principal Actors and Key Entities:



Principal Actors and Key Entities:

General Staff Department Fourth Department

Electronic Countermeasures Department (ECM) Department, oversees both operational ECM units and R&D institutes conducting research on a variety of offensive IW technologies;

General Staff Department Third Department

Signals intelligence (SIGINT) focus, large staff of trained linguists and technicians makes it well suited for oversight of the CND and CNE missions in the PLA; Tasked with the foreign signals collection, exploitation, and analysis and also communications security for the PLA's voice and data networks;

Technical Reconnaissance Bureaus

The PLA maintains at least *six technical reconnaissance bureaus (TRB)* located in the Lanzhou, Jinan, Chengdu, Guangzhou, and Beijing military regions that are responsible for SIGINT collection against tactical and strategic targets and have apparent CNO duties, though few details are available on the exact role or subordination of these units;

Principal Actors and Key Entities:

PLA Information Warfare Militia Units

Since approximately 2002, the PLA has been creating IW militia units comprised of personnel from the commercial IT sector and academia, and represents an *operational nexus between PLA CNO operations and Chinese civilian information security (infosec) professionals;*

→ PLA media reporting indicates that IW militia units are tasked with offensive and defensive CNO and EW responsibilities, psychological warfare, and deception operations, though the available sources do not explain the lines of authority, subordination, or the nature of their specific tasking;

The Chinese Hacker Community

China's hackers, active in thousands of Web-based groups and individually, represent a mature community of practitioners that has developed a rich knowledge
Base: many layers of interest groups: -malware tool developers, legitimate security researchers, hacktivists;

Cyberespionage:

Unclassified foreign government and private sector information, once unreachable or requiring years of expensive technological or human asset preparation to obtain, can now be accessed, inventoried, and stolen with comparative ease using CNO;

→ China is most frequently cited as the primary actor behind much of the activity;

Cyber reconnaissance:

- probing the computer networks of foreign government agencies and private companies;
- identifying weak points in the networks, understanding how foreign leaders think,
- discovering the communication patterns of foreign government agencies and private companies
- attaining valuable information stored throughout the networks;

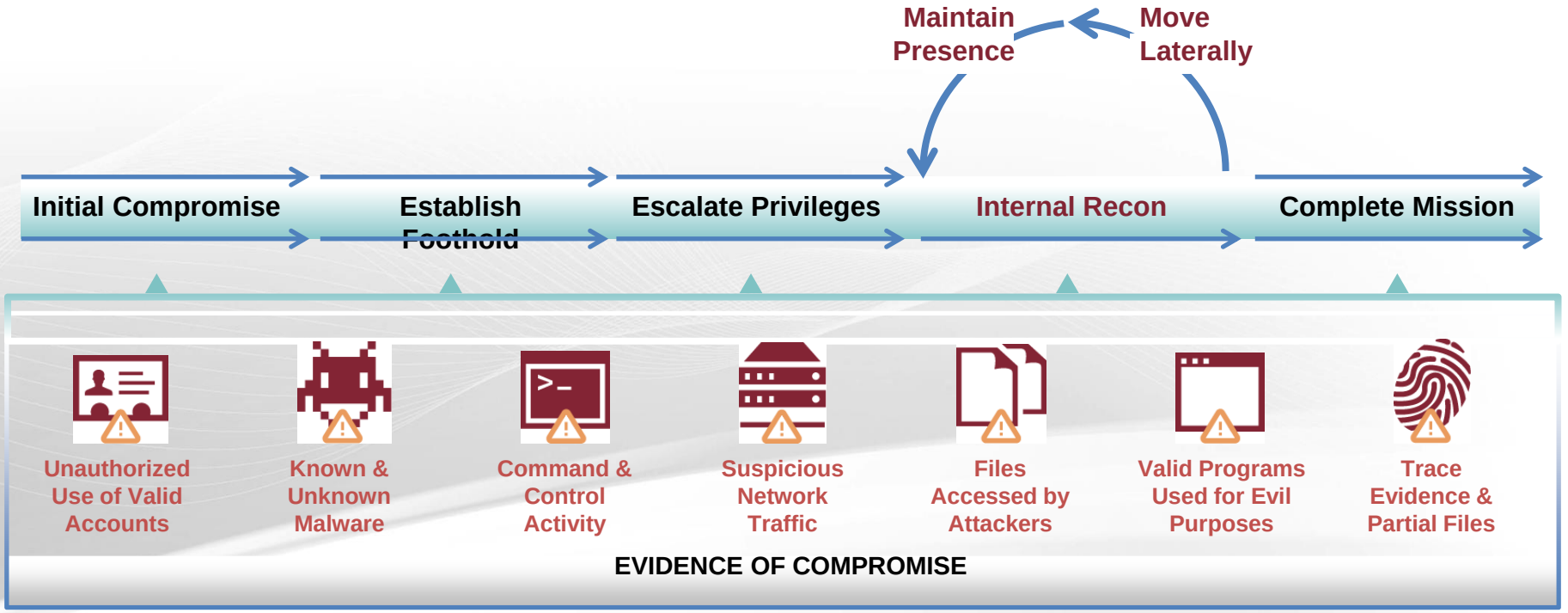
A review of the scale, focus, and complexity of the overall campaign strongly suggest that these operations are state-sponsored or supported.

- access to financial, personnel, and analytic resources that exceed what organized cybercriminal operations or multiple hacker groups operating independently could likely access consistently over several years;

Advanced Persistent Threat:

Mandiant 2013 Report:

Linked APT1 to PLA unit 61398



- Social engineering
- Spear phishing e-mail with custom malware

- Custom malware
- Command and control
- 3rd party application exploitation

- Credential theft
- Password cracking
- "Pass-the-hash"

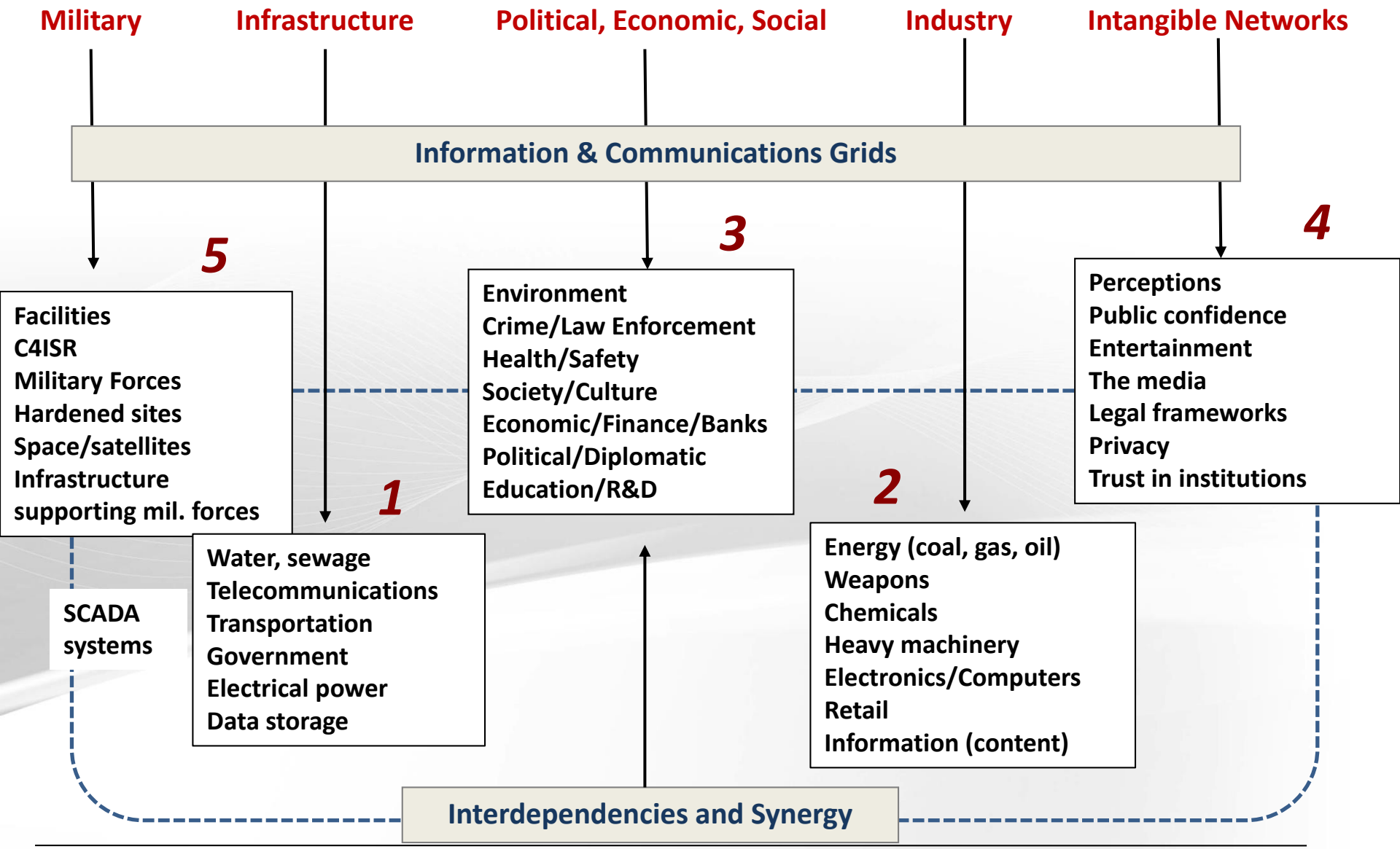
- Critical system recon
- System, active directory & user enumeration

- Staging servers
- Data consolidation
- Data theft

Part 3:

The Future of Cyberwarfare

Weapons of Mass Effectiveness



IW 3.0 Emerging Threat Vectors

	Attacks on computerized systems	Cyber-ops / attacks on physical systems
Cyber Espionage	Attaining intel about the enemy; tactical and operational plans;	Technological, military, business intelligence gathering;
Information Manipulation	Manipulating information in cyberspace;	Perception management Strategic communications Media / Netwars
Confrontations in cyberspace	Attacking enemy computer systems to damage their functions;	Attacks directly affecting the function of devices and systems outside cyber
Wars that include use of cyberspace	All above;	All above;

Source: INSS Even & Siman-Tov

Infrastructure Targets

Water distribution	**(plant, purification, distribution)**
Waste disposal	**(used water, drains, processing)**
Communications	**(POTS, mobile, satellite)**
Road transit	**(streets, roads, highways, buses & trams)**
Train transit	**(regular and underground)**
Air transit	**(passenger and cargo, airplanes, tower control)**
Sea transit	**(cargo, passenger, ship, port control)**

Many of them use SCADA systems:
Supervisory Control and Data Acquisition

i.e. StuxNet atttacks

Many SCADA systems are changing from monolithic (closed network) to distributed (semi open network, proprietary and insecure protocols) to networked systems (open network, secure protocols);

- **Physical intrusion possible to access just *one* endpoint;**
- **Residual threat from insiders;**

Source: Kibin Labs

Attacks Against Satellite Systems

Terra AM-1 was “interfered with” for 2 minutes in June, 2008 and again for 9 minutes October;

Landsat-7 experienced 12 minutes of “interference” in October 2007 and July 2008;

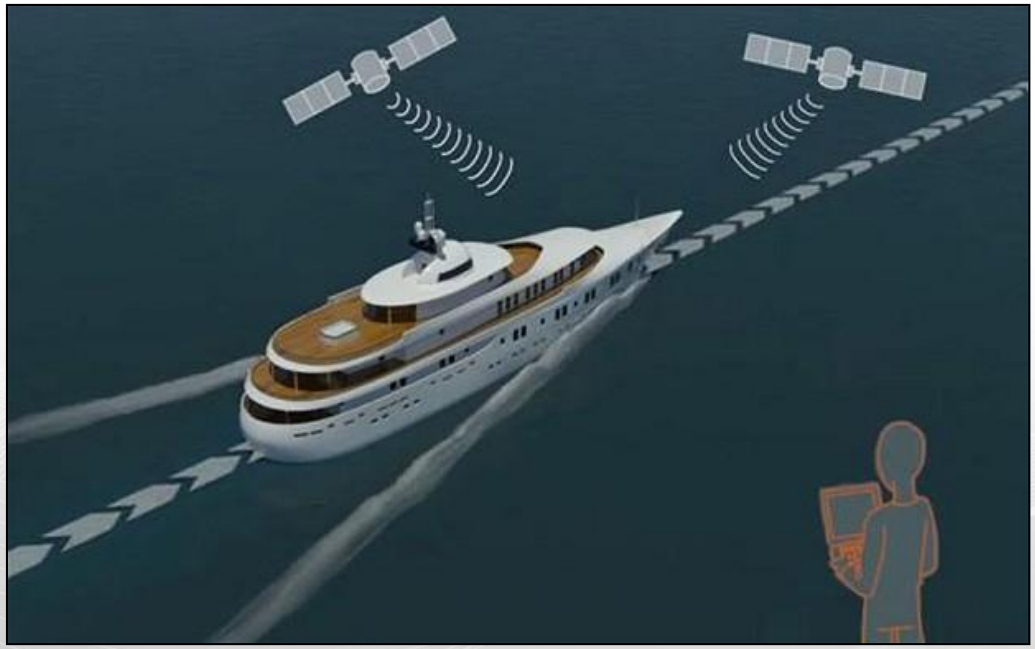
Current satellite systems are vulnerable to several type of attacks:

Denial of Service (Jam Uplink, Overpower Uplink, Jam Downlink)

Attack to Orbital Positioning
Transponder Spoofing,
Direct Commanding,
Command Replay,
Insertion

Dependencies:
Finance
Communications
Transportation
Navigation
Military Espionage/Reconnaissance
News
Weather
Geology
Satellite Internet
TV

GPS Spoofing Attacks



Unlike GPS signal blocking or jamming, spoofing triggers no alarms on navigation equipment;

Broadcasting fake GPS signals from spoofing devices toward ships GPS antennas, slowly overpowering authentic GPS signals until gaining control of the ships' navigation system;

GPS spoofing attacks aren't limited to ships - can be used to attack any system using GPS technology, including aerial defense systems, drones → *MILITARY TARGETS*

Strategic and Policy Implications

- **IW/cyber-warfare is continuously evolving:**

  The scope, magnitude, and impact of IW/CW threats is increasing- from systematic and persistent, to decentralized and dispersed, to accidental and non-malevolent;

  Difficulties in identifying threats, formulating effective responses:
  Who is responsible for IW/cyber defence? Vulnerabilities? Types of response?

- **No country or organisation is immune:**

  Information/cyber security is a complex problem: Governments, corporations, military organizations, and private citizens all depend on technology and information;

- **Different priorities in the development of cyber-warfare capabilities may lead to new balances of power between nation-states and non-state actors;**

Strategic and Policy Implications

- IW/Cyber-warfare will likely play a part in every modern war;
- Cyber security is a process, not a product;
  - multi-level protection
  - information vs. network security
  - advanced cryptography
  - cyber security & monitoring
  - crisis management
  - critical infrastructure protection
  - professional military education
  - research & development
  - funding
  - coordination & oversight