Cyber for CEOs: The Rapid Shift in Hacking and How to Address It

Phillip Hinkle

Director of Cybersecurity and Technology Strategy
Texas Department of Banking

Cyber Threat Assessment

TRAFFIC LIGHT PROTOCOL (TLP): AMBER

Agenda

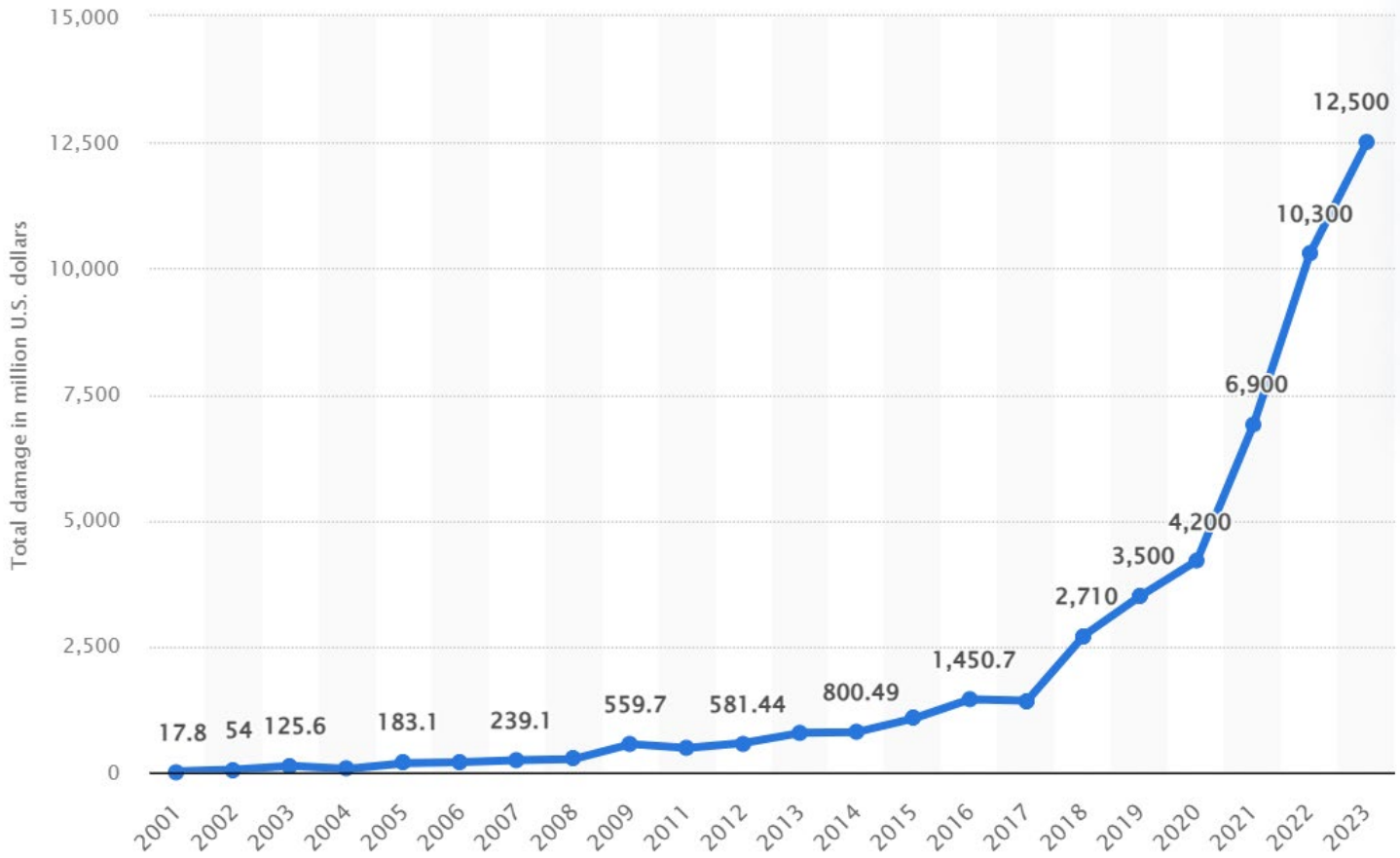
- **Two Biggest Cyber Threats**
  - Ransomware
  - Geopolitical Threat Actors

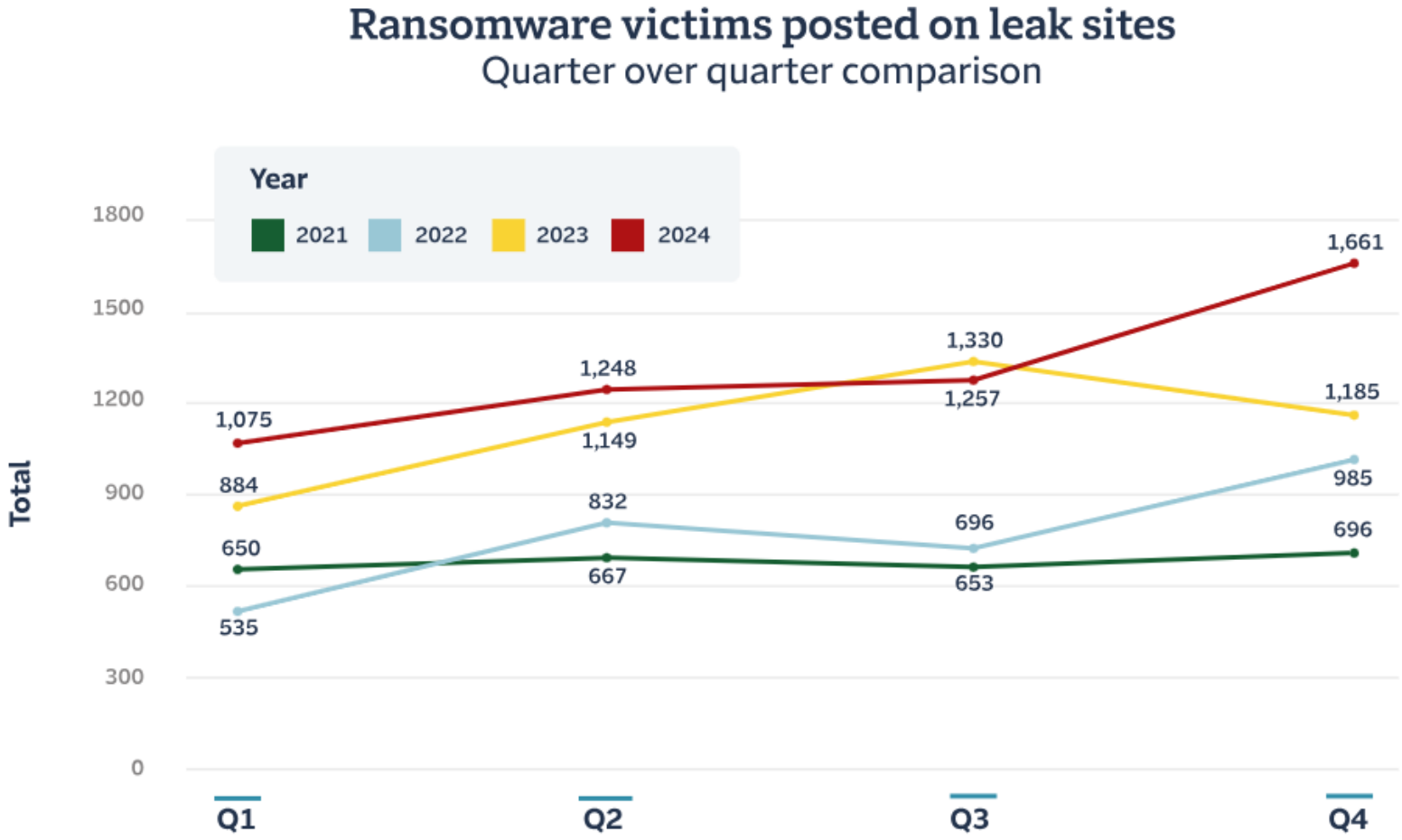
- **Mitigation**
  - Steps To Reduce All Threats

Ransomware

- Continues to be a primary threat
- RaaS – Ransomware as a Service –
  - Any Low Skill Criminal Can Attack You

Zoomable Statistic: Select the range in the chart you want to zoom in on.





Source: Traveler's Insurance Threat Report Q4 2024

Ransomware Trends in 2024

- Activity has trended upward despite disruption in late 2023 / early 2024:
  - LockBit
  - Bianlian
  - Akira
  - 8Base
  - RansomHub
  - Qilin
  - BlackSuit
  - Play
  - Hunters
  - Cactus
- 65 percent of all attacks were carried out by the 10 largest groups
- 55 new groups were noted in 2024

SOURCE: Ransomware 2025: A Resilient and Persistent Threat | Symantec
Q4 Travelers' Cyber Threat Report: Ransomware Goes Full Scale | Corvus

Cyber Insurance Can Help….

- Most policies can include:
    - Breach coach services (forensics & restoration services)
    - Customer notification assistance
    - Call center coordination
    - Customer credit monitoring
    - Data loss/hardware replacement

Ransomware Post-Mortem Study

- Reviewed 55 FIs that were victims
  - 4-year study

- Actions taken after event:
  - Implemented MFA
  - Seriously Completed the RSAT
    (Ransomware Self Assessment Tool)

Ransomware Self Assessment Tool (RSAT 2.0)

- Bank RSAT 2.0.pdf

  (Search for CSBS Ransomware Self Assessment Tool)

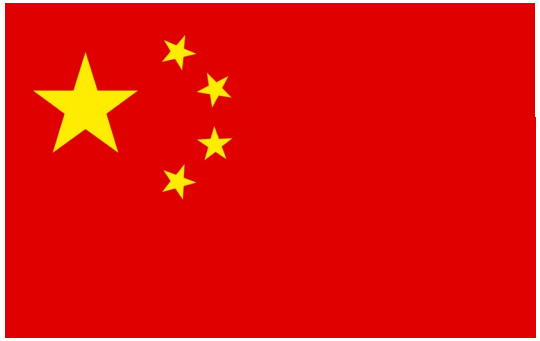
- **Pay particular attention to:**
- **Question #6**

  (Third Parties w/ continuous / intermittent access)

- **Question # 13 (Multi-Factor Authentication)**

Geopolitical Threats

Primary Geopolitical Threat Actors



China

Russia

North Korea

Iran

China Has Our Entire Nation in Their Crosshairs

Testimony Jan 31, 2024

Panelists: FBI Wray;
NSA Director Gen. Nakasone;
CISA Director Easterly; and
National Cyber Director Coker

House Committee Hearing Titled:
THE CCP CYBER THREATS TO THE AMERICAN HOMELAND…

Key Comments Made Regarding China

- **No country presents a *broader*, more *comprehensive* threat to our ideas, our innovation, our economic security, and ultimately, our national security.**

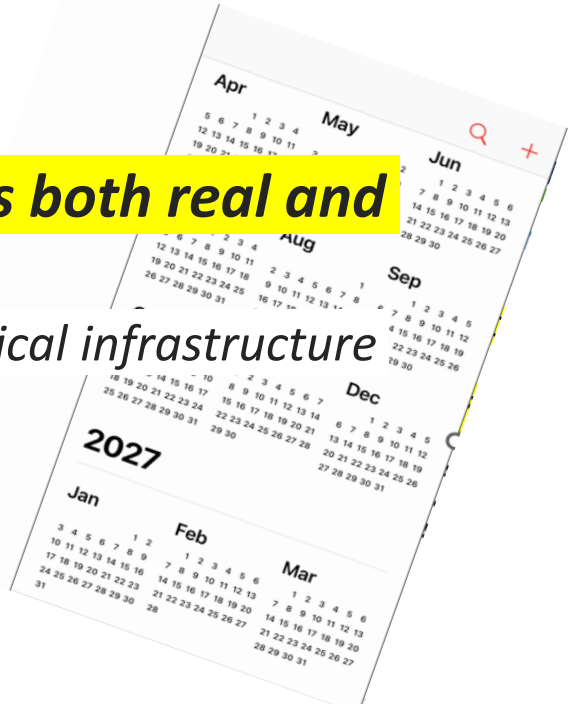
The FBI would be outnumbered 50 to 1 by China if ALL cyber resources were focused on the PRC

Key Comments Made Regarding China (Continued)

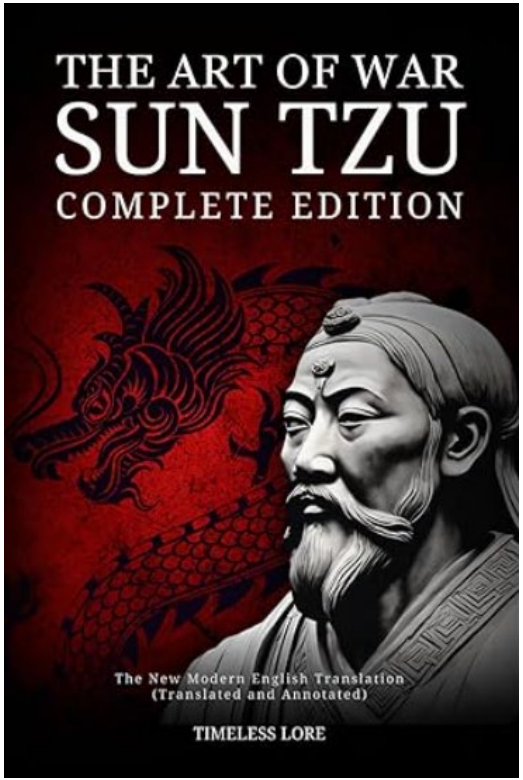
- **[China is] … pre-positioning … to cripple the U.S. <u>in the event China invades Taiwan</u>…**

- ***"This threat is not theoretical… this threat is both real and urgent."***
- *"CISA teams have found ….Chinese intrusions into critical infrastructure across multiple sectors…"*

- **The CCP has 2027 circled on its calendar…"**



2,000-Year-Old Form of Warfare



- Destroy a country by fragmenting people, sowing chaos and distrust

- No appearance of a war.

- In other words:

Disintegration Warfare.

The Smokeless Battlefield

A Peoples' Liberation Army textbook:

"**The battle for mind control happens on a smokeless battlefield.** It happens inside the domain of ideology." "**Whoever controls this battlefield can win** …."

The PRC National Intelligence Law of 2017:

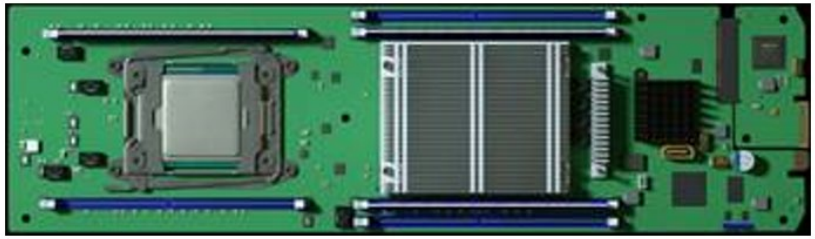
- The Law may be used to compel PRC firms to create backdoors and other security vulnerabilities in equipment and software sold abroad so that the PRC government can easily access data not controlled by PRC firms.

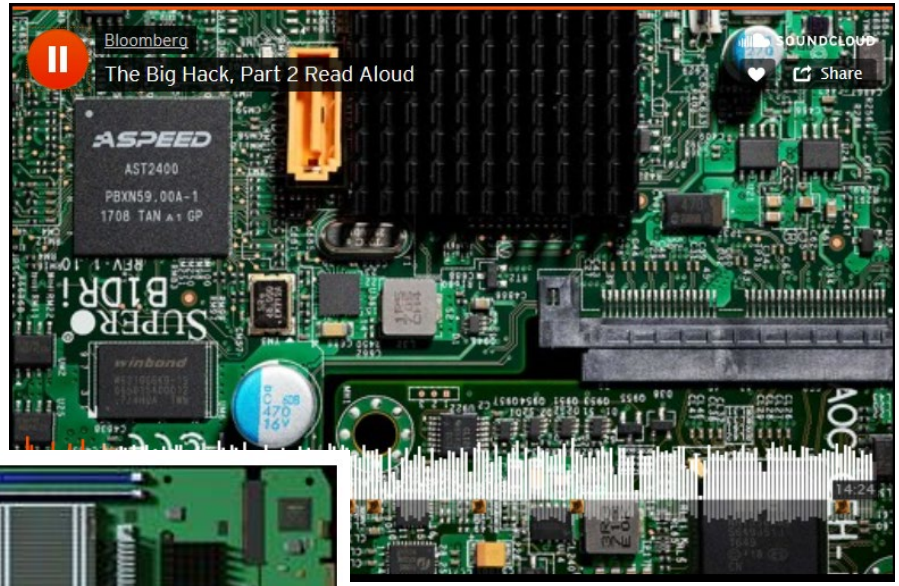
Huawei Banned - Nov 2022

Bloomberg Businessweek

Oct 4, 2018

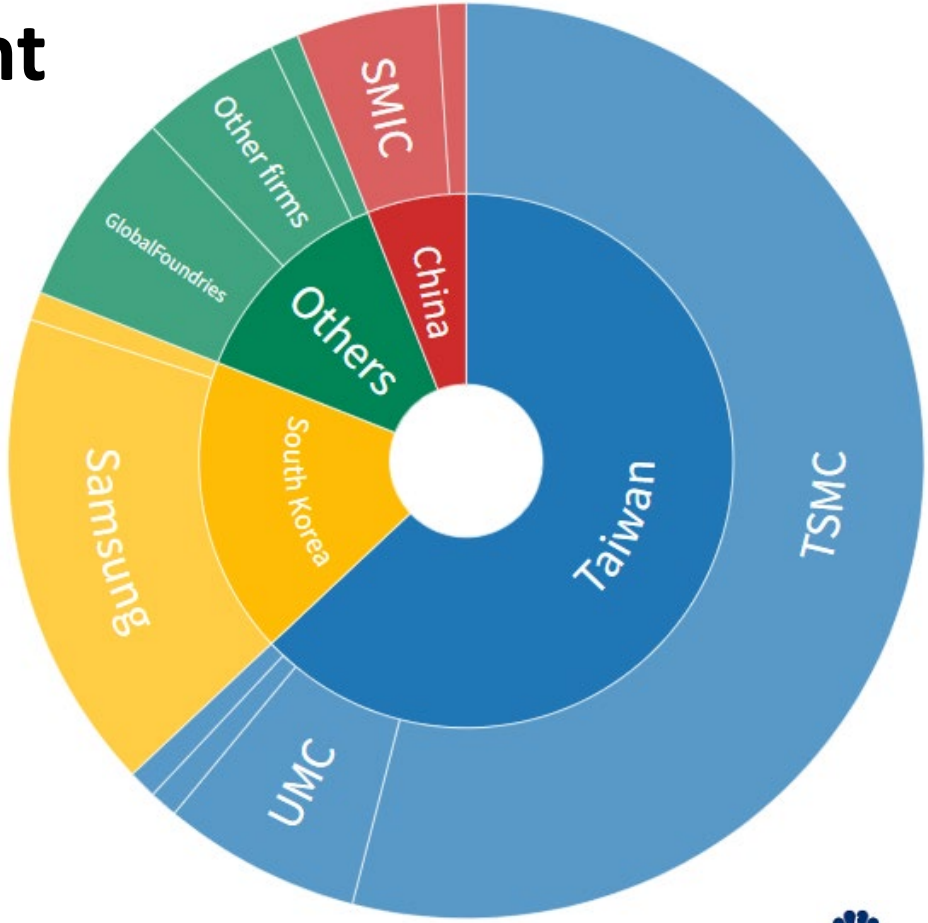
The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies





Why Taiwan is Important to the Free World

Semiconductor Manufacturers by Market Share



Total foundry revenue stood at $85 billion in 2020

SOURCE: TrendForce (March 2021)

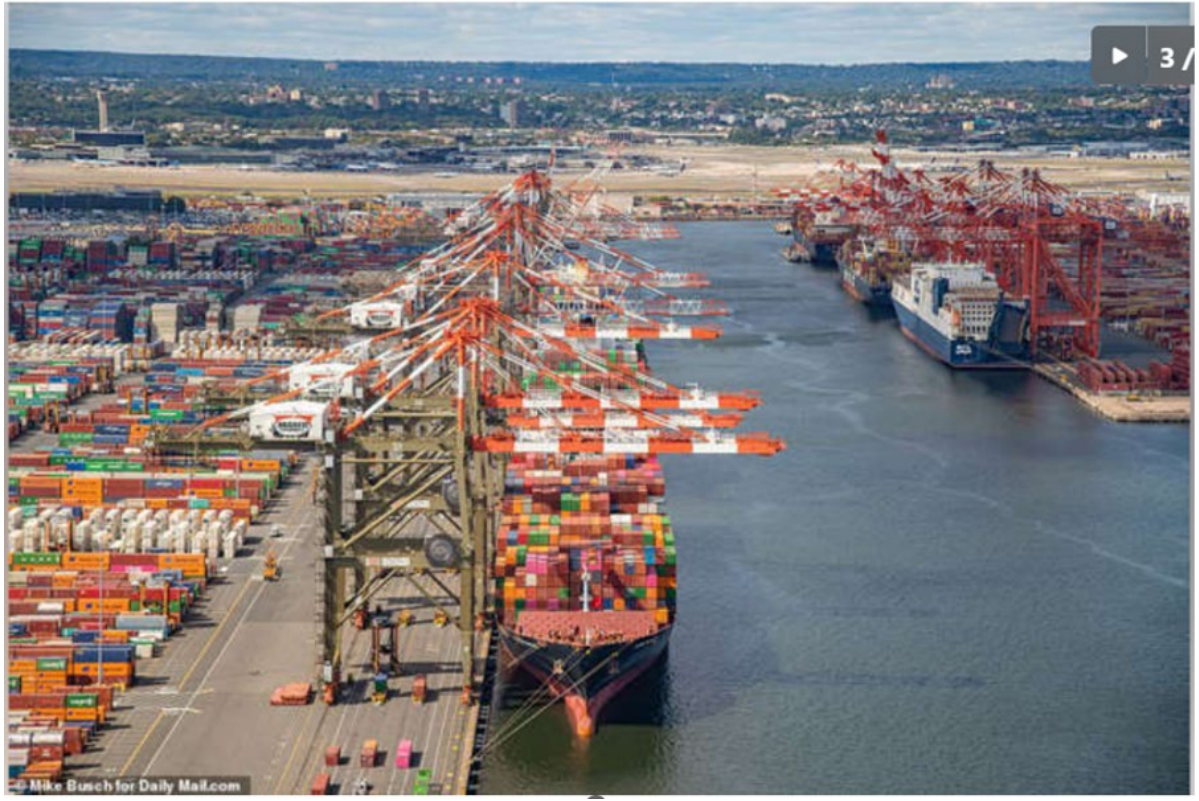
CNBC

American Food Supply and Farmland Being Purchased by China

- China bought Smithfield Farms, the world's largest pork producer.
- Chinese companies have purchased U.S. Agri-chemical plants.
- China has acquired land near critical Air Force bases, including Grand Forks, the backbone of the military's global communication network.
- Four wind farms purchased within U.S. Navy airspace.

Chinese ‘Spy Cranes’ Discovered in U.S. Ports

(with Secret Cellular Internet Connections)



Chinese Medical Devices Could Pose Threat

Backdoors in Chinese-made medical monitors could put patients at risk … according to CISA and the FDA.

The popular Contec CMS8000 patient monitor is an example due to "anomalous network traffic" and a backdoor… that allows "unverified remote files" to be … executed.

This vulnerability could … display false information that might lead to harmful treatment...

Sowing chaos on social media.

We aren't at war with China, but they are at war with us.


11:24
TikTok
Stop a TikTok shutdown
Congress is planning a total ban of TikTok.
Speak up now—before your government strips 170 million Americans of their Constitutional right to free expression.
This will damage millions of businesses, destroy the livelihoods of countless creators across the country, and deny artists an audience.
Let Congress know what TikTok means to you and tell them to vote NO.

Washington Post Warns That China's Hollywood Invasion Is a 'Propaganda' Play

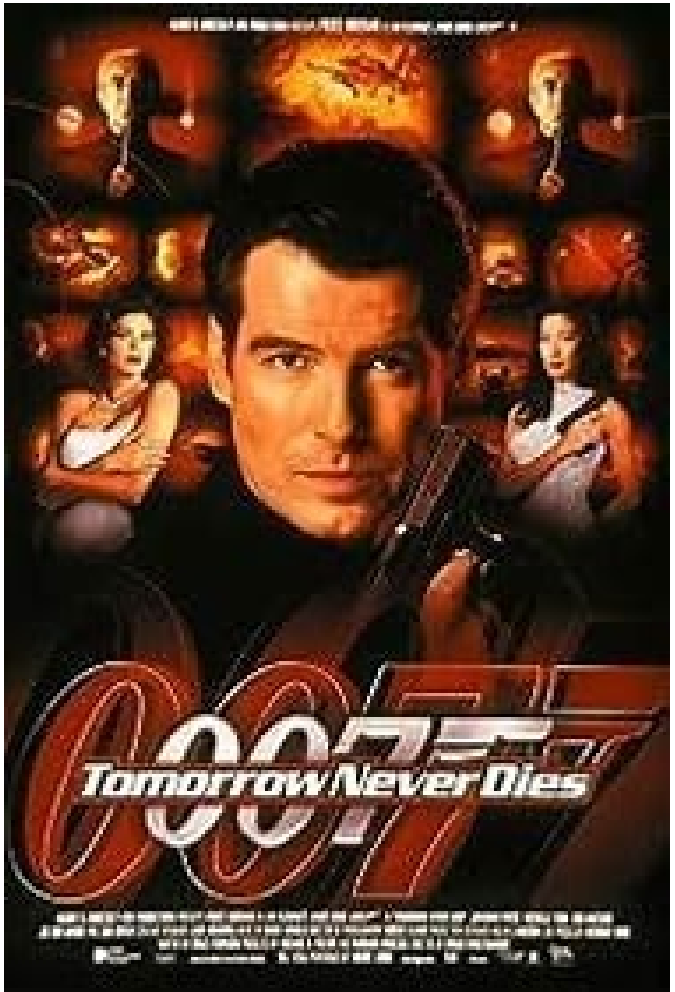
Dalian Wanda Group has bought Legendary Pictures, set a strategic alliance with Sony Pictures and is in talks to buy Dick Clark Productions

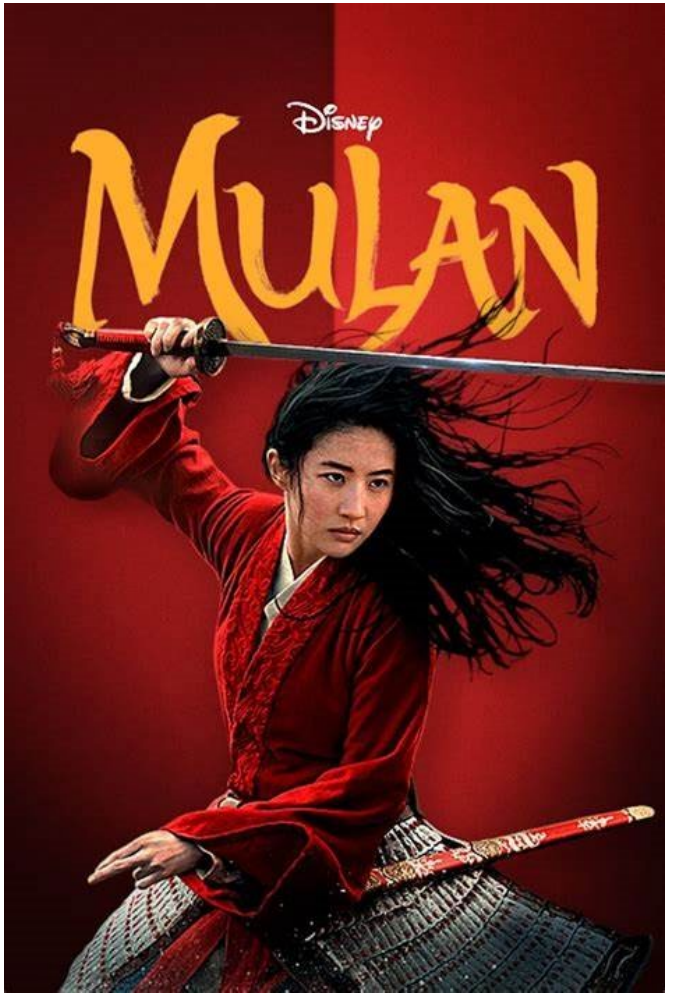
The Wanda Group

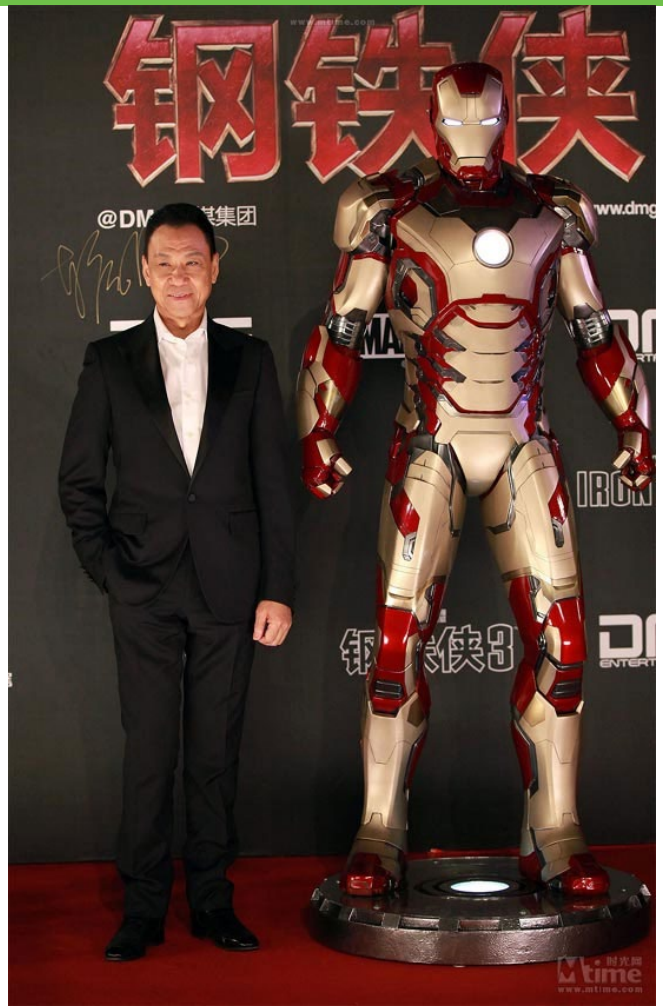
- Owns controlling interest in largest cinema chain in North America.
- If a movie studio wants their movie shown in theaters, it will be reviewed by Chinese censors
- The following movies were all modified to appease censors and show China in a positive light.

Art is a Tool to Further Other Goals

Mao Zedong said: Literature and art are subordinate to politics. Our aim is to ensure that revolutionary **literature and art** … help … facilitating the overthrow of our national enemy….


007
Tomorrow Never Dies


Disney
MULAN

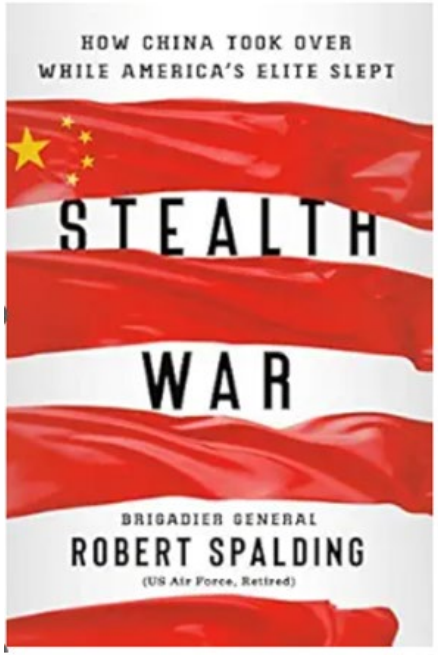

钢铁侠
@DMG传媒集团

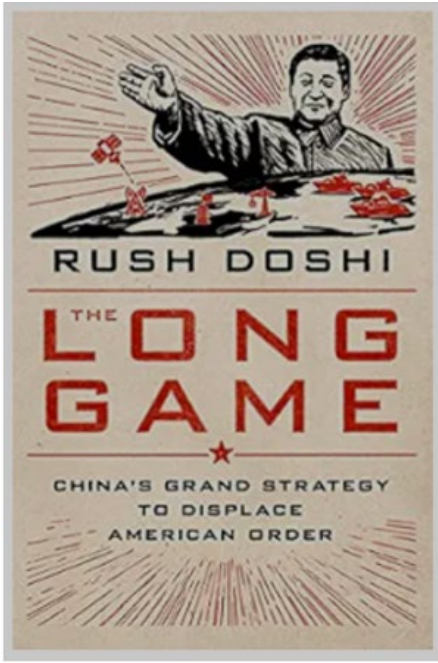

钢铁侠
@DMG传媒集团

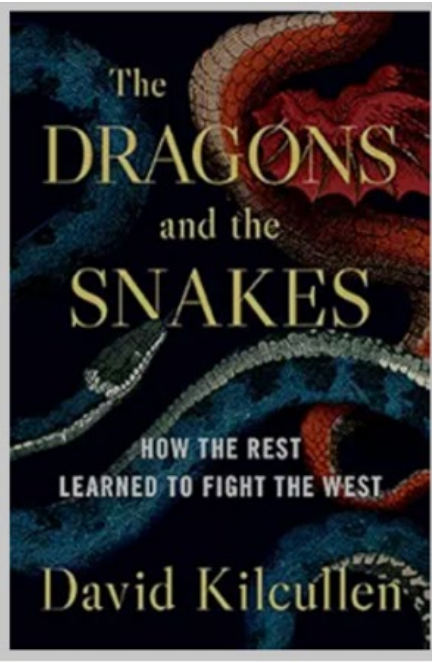
Did 'Barbie' cross the line? How a 'child-like' map stirred a South China Sea dispute

The Japan and Taiwan flags on the jacket were replaced in the 2019 trailer for "Top Gun: Maverick" (right).

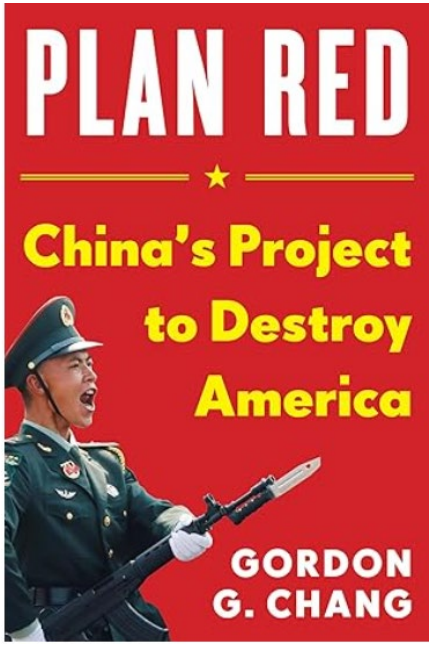
Books on China Threat

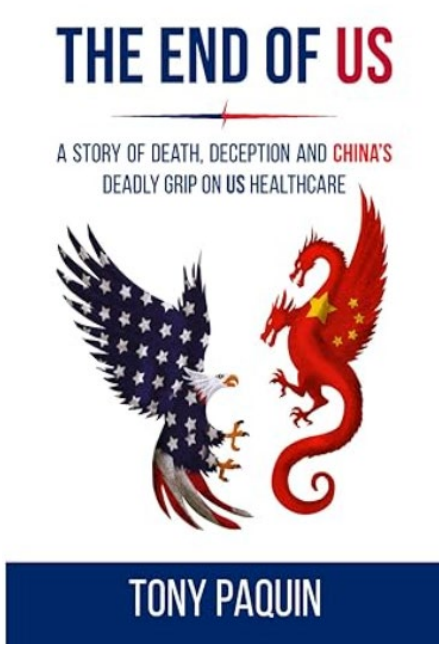


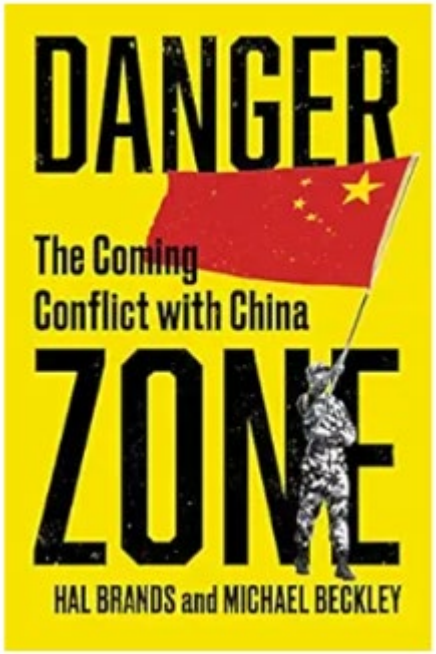


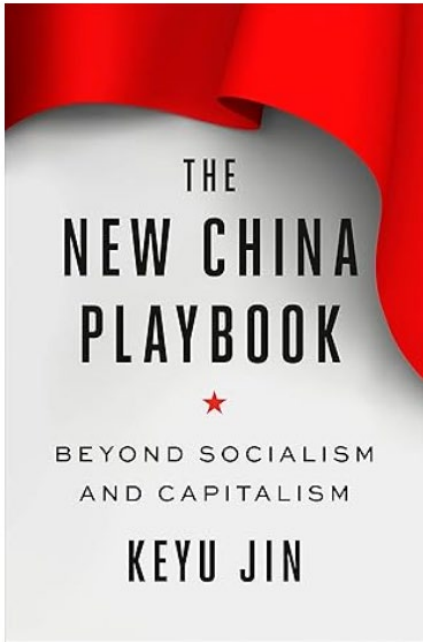


Books on China Threat

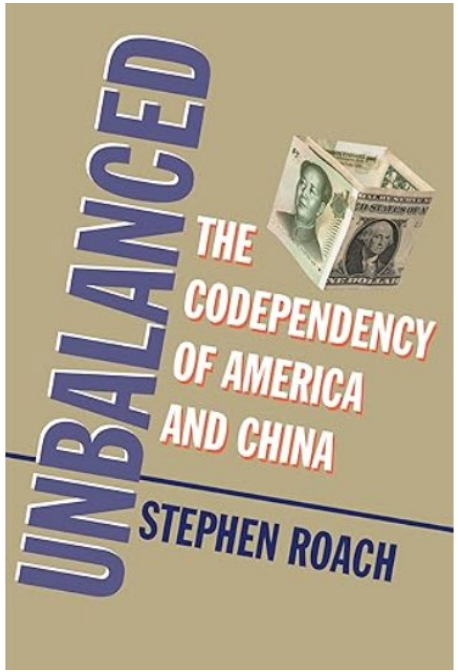


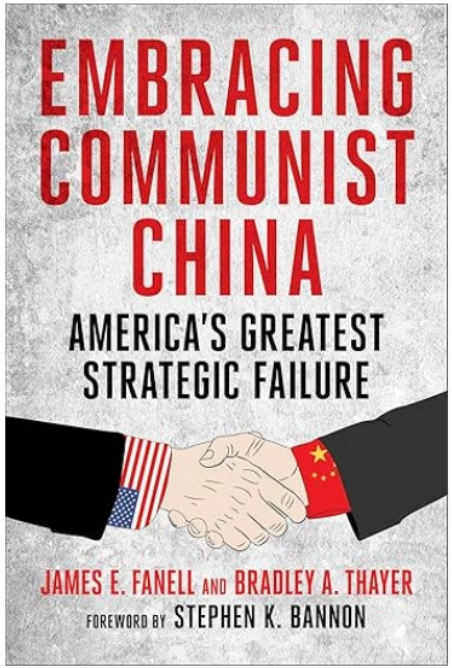


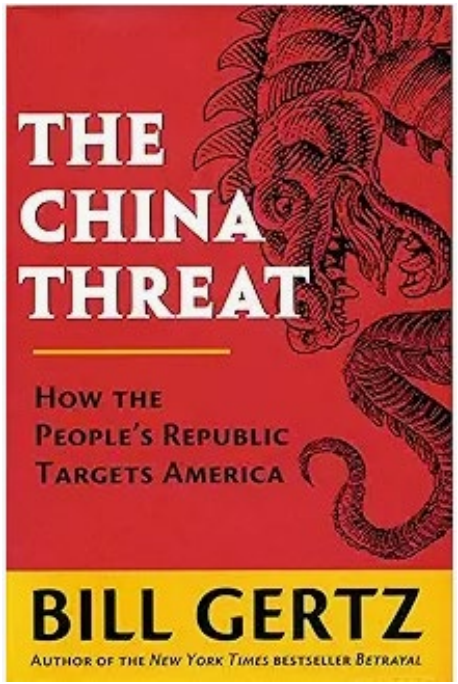


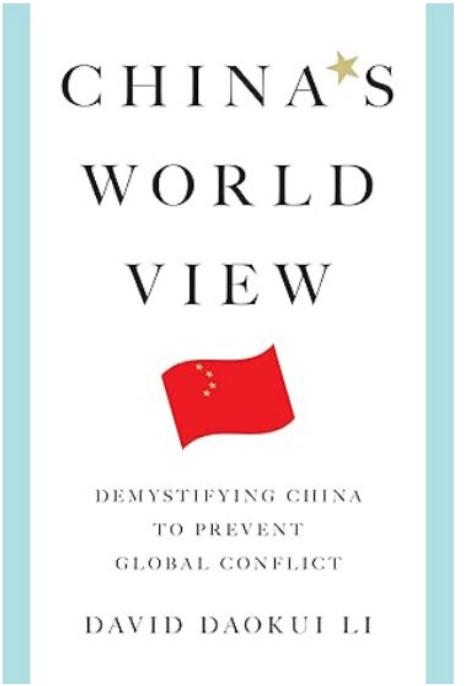


Books on China Threat

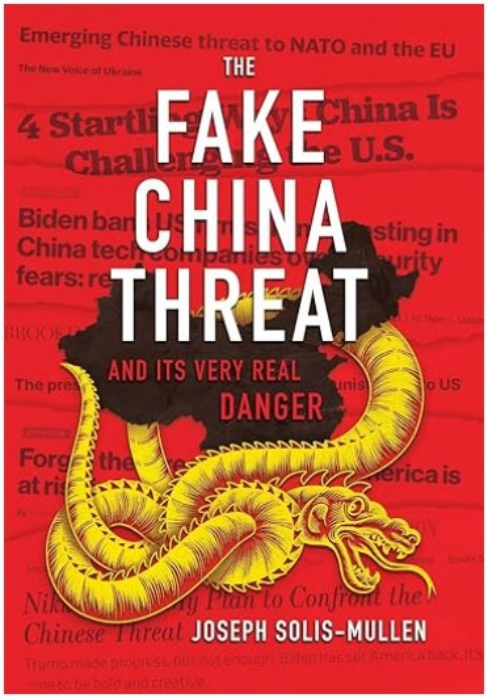


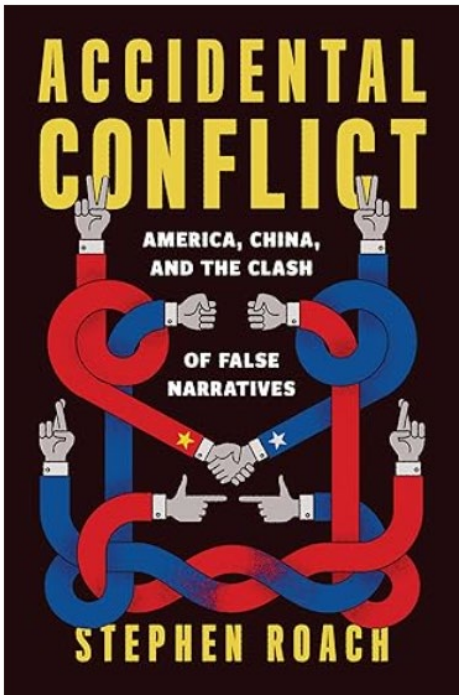


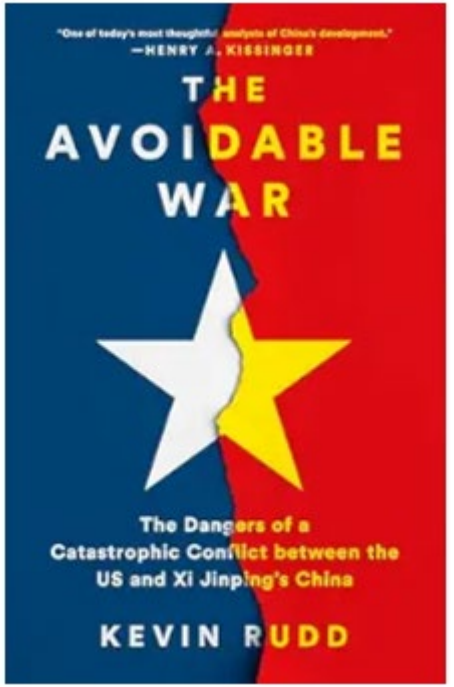




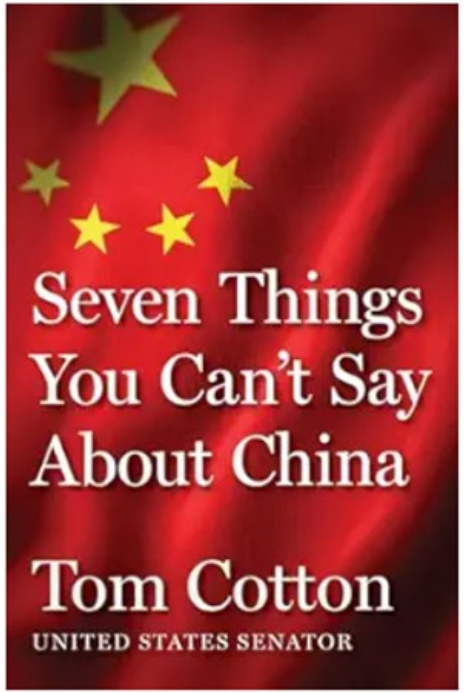
Books Advocating That China Is Not A Threat

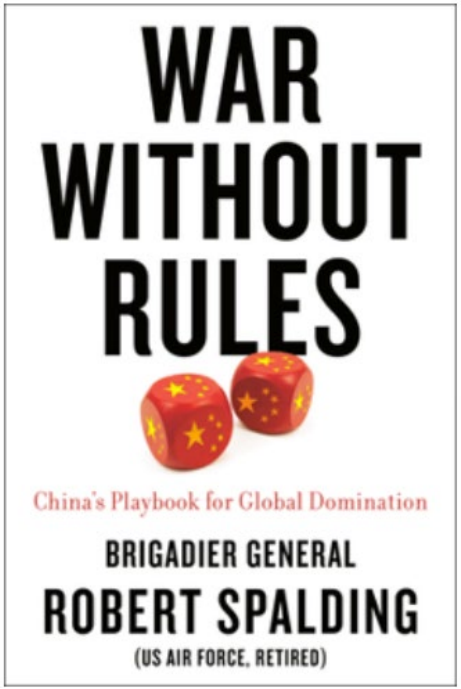


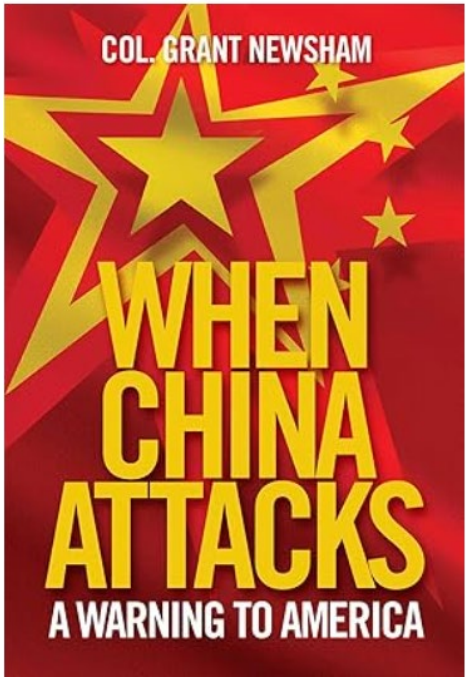




Recommended Introductory Books







Volt Typhoon

- Chinese Cyber Hacking Group pre-positioning in critical infrastructure
- Sole purpose is to enable damage or destruction in the event of a conflict (e.g. invasion of Taiwan)
- To disable or discourage our ability to respond to invasion

Volt Typhoon active since 2021:

- Activity, however, was only discovered in May 2023
- Overshadowed by MOVEit, which occurred simultaneously

What Can We Do?

National security agencies must continue to

- Continued awareness on recommended actions for network operators to find and prevent malicious access to networks

- Make it harder for China to compromise our networks.

Volt Typhoon Employs “Living Off The Land” (LOTL) Techniques

- Use of legitimate network tools to perform malicious activities
- Avoids detection – blends in with normal activity
- LOTL benefits from limited network logging in default configurations


TLP:CLEAR
ASD
AUSTRALIAN SIGNALS DIRECTORATE
ACSC
Australian Government
Australian Signals Directorate
Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité
National Cyber Security Centre
PART OF THE GCSB
National Cyber Security Centre
a part of GCHQ
JOINT GUIDANCE:
Identifying and Mitigating Living Off the Land Techniques
Publication: February 7, 2024
U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency


Best practices for event logging and threat detection

Basic Technique of Volt Typhoon

- **Privileged Access Credentials are gathered***

  - Targets individual employees
  - Monitors individual employees' personal social media
  - China (and North Korea) targets Managed Service Providers (MSPs)

*2024 Verizon Data Breach Report cited credential compromise in nearly 40% of all intrusions.

Cyber Hygiene

"Basic cyber hygiene prevents 98% of cyber attacks"

– Former CISA Director Jen Easterly

- Cyber hygiene programs are well-known controls
- BUT, often they are not *consistently implemented and managed*

CISA Recommendations

(Focus on reducing compromises of privileged access)

ACTIONS TO TAKE TODAY TO MITIGATE VOLT TYPHOON ACTIVITY:

1. Apply patches for internet-facing systems. Prioritize patching critical vulnerabilities in appliances known to be frequently exploited by Volt Typhoon.
2. Implement phishing-resistant MFA.
3. Ensure logging is turned on for application, access, and security logs and store logs in a central system.
4. Plan “end of life” for technology beyond manufacturer’s supported lifecycle.

MFA - Use On All Privileged Access

- Domain administrative access
- Access to any Cloud-based services
- Third Party Access (like MSPs)
- All VPN / RDP access

CISA's Cyber – Hygiene (CyHy)

- **Does *NOT* Give the Government "Network Access"**

- Free Weekly Vulnerability Scans of *Edge Devices*
- Provides Insight of *Industry* Vulnerabilities
- Can Help Provide Rapid Industry Alerts of Exploitation

PRESIDENTIAL ACTIONS

Achieving Efficiency Through State and Local Preparedness

The White House | March 19, 2025

IT Examinations

- IT exam frequency developed before the Internet
- IT threats changed very little from decade to decade
- Cyber threats evolve at Internet speed now, but exam cycle remains the same.
- **Mile Wide, but Only an Inch Deep --- Need the Reverse**

Thoughts on IT Exam Modernization

- The current threat is real and urgent;
- IT Exam Cycle should be Agile and Timely
  - Reviews Needed of Emerging Threats
  - Scale Exam Down to Riskiest Areas
  - IT Audits Too Weak to be Leveraged
  - Industry and regulators need to work together

Call to Action

- Implement the Four Priority Controls Outlined by CISA
- Use the Ransomware Self Assessment Tool
- Speak to your business customers … and civic organizations about the threat China poses
- Talk to your core service provider

Closing Thoughts – It is not all Gloom and Doom

- China is not omnipotent– It has significant internal weaknesses
  - There are only 5 *surviving* communist countries
  - China is the oldest at 75 years

- The Soviet Union led the Space Race
- However, the Soviet Union Doesn't Exist Today
- U.S. won the Space Race – and landed on the Moon (and ultimately won the Cold War)

Questions / Comments