gocyber

COLLECTIVE

Information

Feel free to email us at Admin@gocybercollective.org.

If you have a suggestion on meeting topics, special interest groups, breakfast menu, or anything else we want to hear from you.

You can register and download past presentations from the website.

- GoCyberCollective.org

Event Sponsors

SECURECYBER
DEFENSE

FORTINET®

Cybersecurity Threat Update

The Last 2 Weeks in Cyber

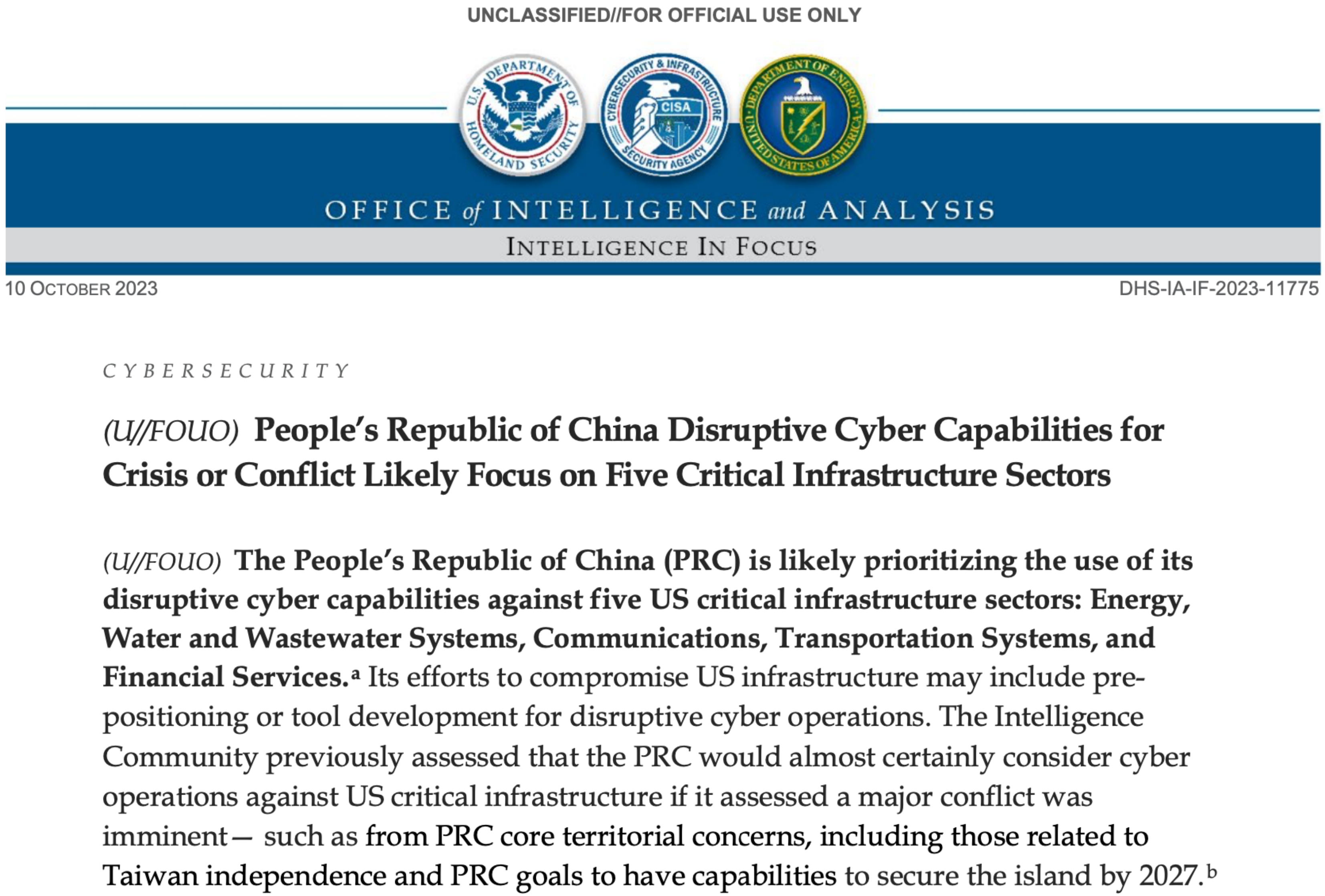
- Conti/Royal/LockBit Very Active
- VMware Vulnerabilities
- GootLoader Malware Active
- Fortinet Vulnerabilties – Client/Gate
- Okta - Multiple Compromises

The Last 2 Weeks in Cyber

Microsoft – 3 Vulnerabilities Active Exploit

Critical Cisco Vulnerabilities

Citrix NetScaler



UNCLASSIFIED//FOR OFFICIAL USE ONLY

OFFICE *of* INTELLIGENCE *and* ANALYSIS

INTELLIGENCE IN FOCUS

10 OCTOBER 2023

DHS-IA-IF-2023-11775

CYBERSECURITY

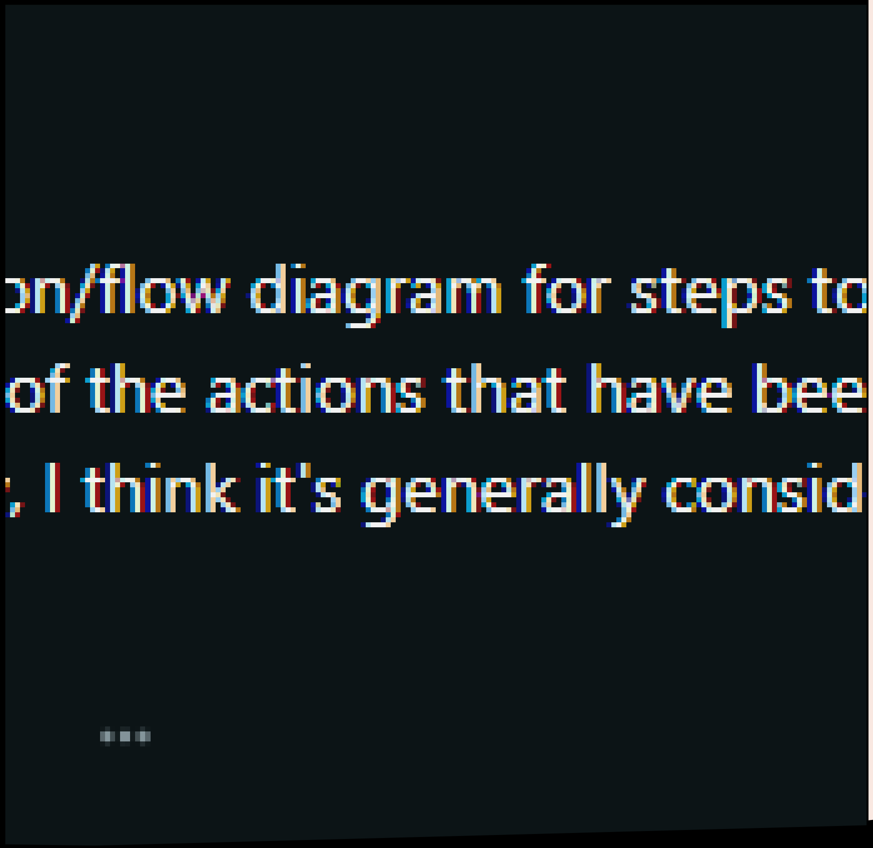
(U//FOUO) People's Republic of China Disruptive Cyber Capabilities for Crisis or Conflict Likely Focus on Five Critical Infrastructure Sectors

(U//FOUO) **The People's Republic of China (PRC) is likely prioritizing the use of its disruptive cyber capabilities against five US critical infrastructure sectors: Energy, Water and Wastewater Systems, Communications, Transportation Systems, and Financial Services.**[a] Its efforts to compromise US infrastructure may include pre-positioning or tool development for disruptive cyber operations. The Intelligence Community previously assessed that the PRC would almost certainly consider cyber operations against US critical infrastructure if it assessed a major conflict was imminent— such as from PRC core territorial concerns, including those related to Taiwan independence and PRC goals to have capabilities to secure the island by 2027.[b]

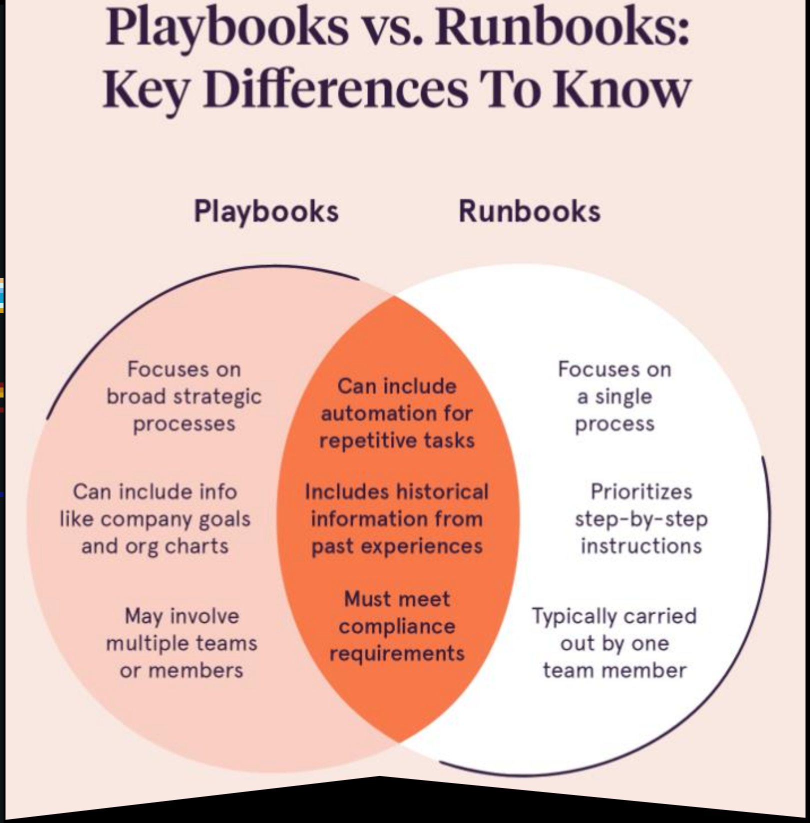
Shawn’s Top Recommendations

1. Install EDR Immediately
2. Setup a Syslog Server/SIEM
3. Remove RDP Access Externally
4. Address Your Backup Status
5. Patch Often
6. Segment Your Network
7. Move VLANS to the Firewall
8. MFA on O365 – Everyone
9. Use Web Filtering
10. Use Intrusion Prevention (IPS)
11. Use a Robust Email Filter
12. Train Your Users! – Often
13. Use Quarantine Features

Playbooks



on/flow diagram for steps to
of the actions that have bee
, I think it's generally consid



Playbooks vs. Runbooks: Key Differences To Know

Playbooks

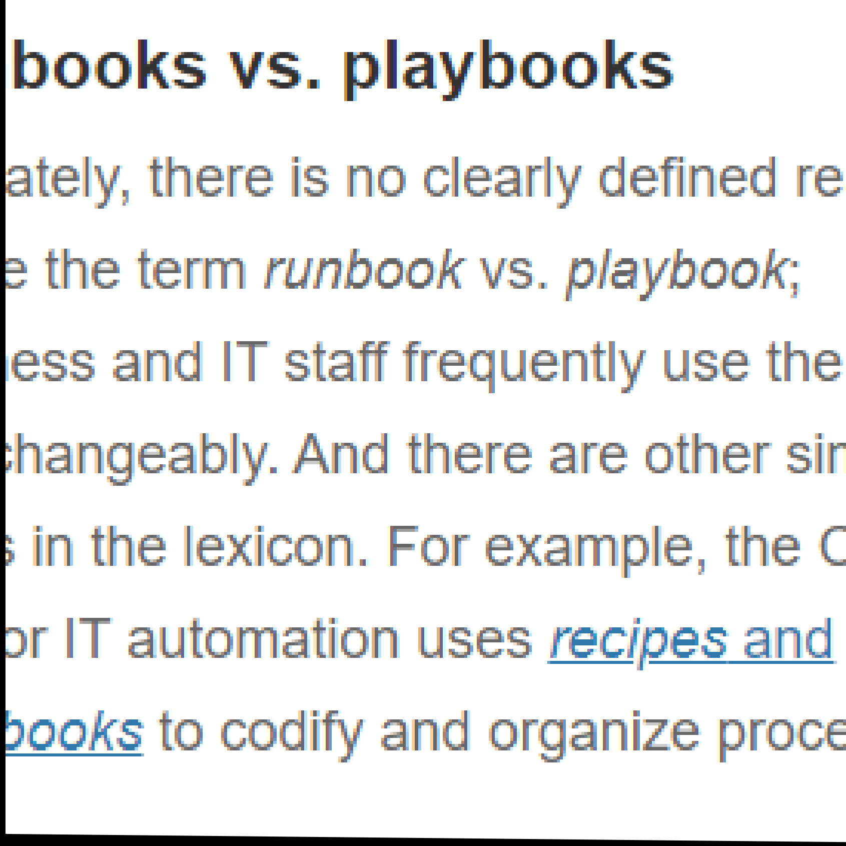
- Focuses on broad strategic processes
- Can include info like company goals and org charts
- May involve multiple teams or members

Playbooks and Runbooks

- Can include automation for repetitive tasks
- Includes historical information from past experiences
- Must meet compliance requirements

Runbooks

- Focuses on a single process
- Prioritizes step-by-step instructions
- Typically carried out by one team member



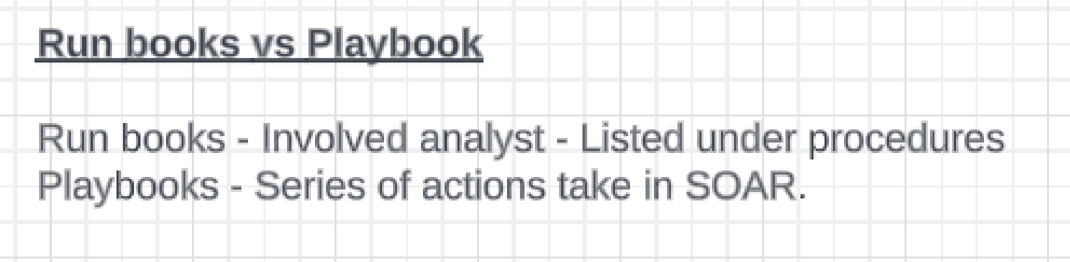
books vs. playbooks

ately, there is no clearly defined re
e the term *runbook* vs. *playbook*;
ess and IT staff frequently use the
hangeably. And there are other sir
s in the lexicon. For example, the C
or IT automation uses *recipes and*
books to codify and organize proce

https://www.tango.us/blog/playbook-vs-runbook#:~:text=Runbooks%20are%20your%20go%2Dto,to%20document%20more%20complex%20processes

https://www.reddit.com/r/CompTIA/comments/13ri1te/playbooks_vs_runbooks_difference/

https://www.techtarget.com/searchitoperations/tip/Compare-runbooks-vs-playbooks-for-IT-process-documentation



Run books vs Playbook

Run books - Involved analyst - Listed under procedures
Playbooks - Series of actions take in SOAR.

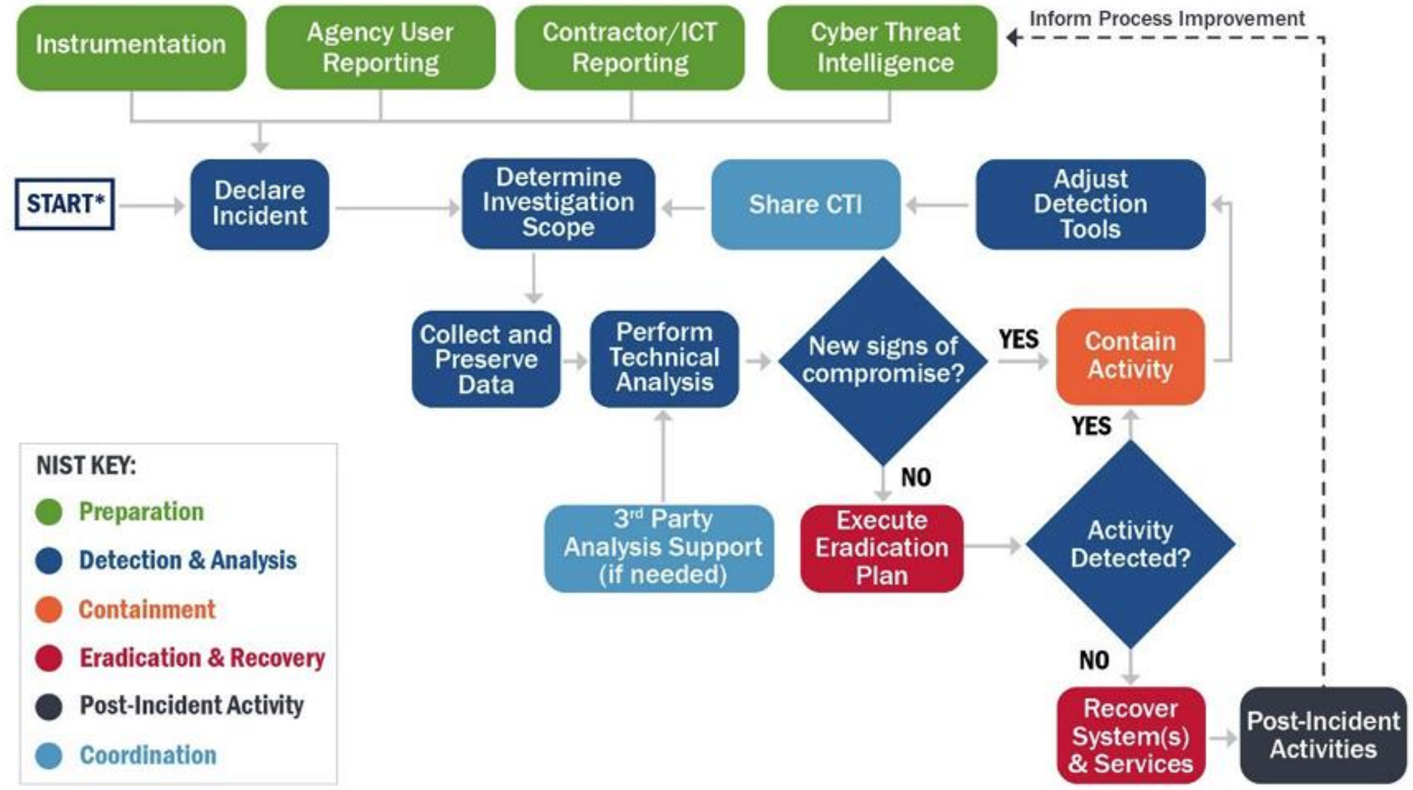


Figure 1: Incident Response Process

https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

- No trial by fire
- Controlled exposure
- Identify gaps
- Predictable and consistent results

What next?

- Identify Risk
- Develop playbook / runbook
- Implement and train
- Continuous improvement

Resources

- Microsoft –
  https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks
- Google –
  https://inthecloud.withgoogle.com/top-security-playbooks/on-demand.html
- Incident response samples –
  https://www.incidentresponse.org/playbooks/

gocyber

COLLECTIVE