Cross-Cultural Uses of Cyber Threat Intelligence

Marty Green—Montana State University
Mentors: Dr. Clemente Izurieta & Yvette Hastings

Introduction

Since the late 2000s, cyber capabilities have become a central instrument of national power. States increasingly integrate cyber operations into military doctrine, intelligence collection, economic competition, and political influence campaigns. However, national cyber strategies differ significantly depending on political systems, strategic culture, and resource constraints. Some states emphasize espionage and intellectual-property theft, while others prioritize information warfare, financial cybercrime, or disruptive attacks on infrastructure.

Major state cyber actors commonly examined in threat-intelligence reports include the United States, Russia, China, Iran, and North Korea, each demonstrating distinct patterns of cyber activity and doctrine. Understanding what tendencies governments have can allow us to better equip ourselves.

Methods

A literature review was conducted using the search string 'state sponsored cyber-security', state cyber doctrine', and 'cyber attacks' between 2008-present on Google Scholar. Search criteria was: is the paper about cyber capabilities/ does the paper have multiple authors/is it from the 2000s/ is the paper's topic directly related to national cyber doctrine. After criteria was met, I focused on about 30 abstracts of which I read 20 papers and used 11 in this project.

State Comparisons[1,2,3,4,5,8,10,11]

Russia:
- Emphasizes disruption + hybrid warfare
- Integrates cyber with:
  - Information warfare
  - Psychological operations

Western states (U.S. and allies):
- Precision cyber operations
- Integration with conventional military strategy

China:
- Long-term cyber espionage
- Strategic accumulation of data and intellectual property

North Korea:
- Financial cybercrime
- Political retaliation

Iran:
- Regional influence and disruption
- Political retaliation

State Cyber Operations[5,6,7,9,11]

Op Type	Description	Example
Cyber Espionage	Theft of Intel or intellectual property	Chinese APT campaigns
Infrastructure Disruption	Attacks on utilities or transport systems	Ukraine power grid attack
Info Warfare	Political influence or disinformation	Russian election interference
Financial cybercrime	Theft or ransomware to generate revenue	North Korean crypto theft
Supply Chain Attacks	Compromise of software distribution systems	SolarWinds Attack

Challenges[6,7,8,9,10]

Limits of Attribution
- Cyber attacks can be rerouted (botnets, proxy servers)
- Attackers can reuse or mimic malware signatures
- Evidence is circumstantial rather than definitive
- Designed operations can:
  - Imitate others' tactics
  - Plant misleading codes or language markers
- Political aversion to publicly assign blame (delays, withholding evidence)

Normative and Legal Gaps
- Definitions of "cyberattack" and "cyberwar" are unclear
  - Unclear threshold of damage to justify self-defense
  - Legal-grey zone
  - Guidelines are non-binding
- Infrastructure has no universally enforced rules
- Lack of enforcement mechanisms
- State Prioritization differs
- Rapid technological advances and changes, slow legal adaptations

Defense Implications[1,2,5,7,11]

- International cyber norms are heavily underdeveloped
- Critical infrastructure must be prioritized
- Threat detection is fragmented and reactive
- Improved attribution mechanisms are needed to identify responsible actors
- Reduced consequences impact deterrence abilities

Conclusion

Since 2008, cyber operations have become a fundamental component of national strategy. States employ cyber capabilities in ways that reflect their political priorities, strategic cultures, and resource limitations. Western powers tend to focus on precision cyber operations integrated with military strategy, while countries such as Russia and Iran emphasize disruptive attacks and hybrid warfare. China prioritizes long-term espionage, and North Korea relies on cybercrime to support its economy. Understanding these national patterns is essential for anticipating cyber threats, strengthening defensive strategies, and developing international frameworks capable of managing cyber conflict in an increasingly interconnected world. In order to better combat others, we must understand their tendencies and attack/defense preferences.

Acknowledgements

This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute.

References

[1.]Aviv, I., & Ferri, U. (2023). Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. *International Journal of Critical Infrastructure Protection, 43*, Article 100637. https://doi.org/10.1016/j.ijcip.2023.100637 ScienceDirect
[2.]Durojaye, H., & Raji, O. (2022). Impact of state and state-sponsored actors on the cyber environment and the future of critical infrastructure. *arXiv*. https://arxiv.org/abs/2212.08036 arXiv
[3.]Finlay, C. J. (2018). Just war, cyber war, and the concept of violence. *Philosophy & Technology, 31*, 357–377. https://doi.org/10.1007/s13347-017-0299-6 SpringerLink
[4.]Finlay, L., & Payne, C. (2019). The attribution problem and cyber armed attacks. *American Journal of International Law, 113*, 202–206. https://doi.org/10.1017/aju.2019.35 Cambridge University Press
[5.]Giles, K. (2023, December 14). Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine. *Chatham House*. https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice
[6.]Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122 Taylor & Francis Online
[7.]Orleans-Bosomtwe, P. K. (2024). Critical infrastructure security: Penetration testing and exploit development perspectives. *arXiv*. https://arxiv.org/abs/2407.17256
[8.]Rid, T. (2013). *Cyber war will not take place.* Oxford University Press
[9.]Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defense Centre of Excellence.* Cambridge University Press. https://guides.ll.georgetown.edu/cyberspace/cyber-conflicts
[10.]Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press
[11.]U.S. Department of Defense. (2018). *Department of Defense cyber strategy.* U.S. Government Publishing Office. https://dod.defense.gov/Portals/1/Documents/pubs/2018-Cyber-Strategy-Summary.pdf