The Cyber Frontier of Political Warfare:

How States Use Cyber Operations to Influence and Destabilize Political Systems

W. KALAB STEPHENSON | VICEROY NORTHWEST INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH

INTRODUCTION

The "Cyber Frontier" has replaced the physical battlefield as the primary arena for modern political warfare. State actors like Russia, China, and Iran no longer rely solely on military force; instead, they utilize digital tools to destabilize adversaries from within. By integrating disinformation, hacking, and narrative control, these states can erode public trust and influence political outcomes with minimal cost and high deniability. This study compares these three distinct state strategies to demonstrate how cyber operations have become the central pillar of 21st-century destabilization.

Although different than traditional warfare, cyber attacks pose a real threat through psychological attacks which harm state credibility and spread misinformation.

Figure 1. Disinformation is now part of mainstream politics. Photo by iStock, 2025. Reprinted with permission from NordForsk.

METHODOLOGY

This research uses a comparative case study approach to draw conclusions about the cyber methods foreign actors use to destabilize states:

- **Scope:** The study analyzes the cyber doctrines and recorded operations of Russia, China, and Iran between 2020 and 2026, to determine the impacts these states have on international politics through cyber operations.
- **Data Collection:** Data is drawn from a peer-reviewed journal, 4 think-tank reports (CSIS, Carnegie Endowment, Aspen Institute Germany, and Council on Foreign Relations), a relevant news article, FBI most wanted page, and a policy brief.
- **Analysis:** The study applies content analysis to identify patterns in state-sponsored messaging and policy analysis to evaluate the effectiveness of international responses.

RESULTS/ FINDINGS

- **Low Barrier to Entry:** Unlike traditional military hardware, cyber tools are affordable. This allows states with smaller economies to participate in conflicts.
  - Despite its smaller economy, Iran used the Shamoon cyberattack to wipe and “brick” 35,000 hard drives at Saudi Aramco, paralyzing the world’s largest oil company for weeks. This remains one of the most destructive examples of how a mid-sized power can use low-cost digital tools to inflict massive economic damage on a global giant.
- **The "Gray Zone" Advantage:** Designed to stay below the threshold of armed conflict. Because attribution is difficult, states can interfere in elections or spread disinformation with minimal risk of physical retaliation.
  - In 2016, Russian military intelligence executed a 'hack-and-leak' operation against the DNC, utilizing stolen private communications in a attempt to influence the elections.
- **Psychological Impact:** The most successful operations do not destroy hardware; they destroy public trust. By spreading contradictory narratives, states effectively polarize target populations and weaken democratic institutions
  - We can see this today in the United States, where political extremism is disseminated by foreign actors to sew division where normally there would be normal political discourse within the United States. (See Figure 2)

CONCLUSION

Cyber operations have become a central pillar of modern political warfare. This study concludes that states such as Russia, China, and Iran use these tools because they are cost-effective and provide plausible deniability. The primary goal is the breakdown of trust in government and the destabilization of political narratives. To counter these threats, future policy must move beyond technical defense and focus on building societal protection against psychological manipulation. in practice, this could mean including digital literacy into public education to ensure citizens can identify and neutralize state-sponsored disinformation before it takes root.

DISINFORMATION FROM GOVERNMENTS

Disinformation is used to psychologically manipulate individuals of competing states but also used to influence their own domestic narrative.

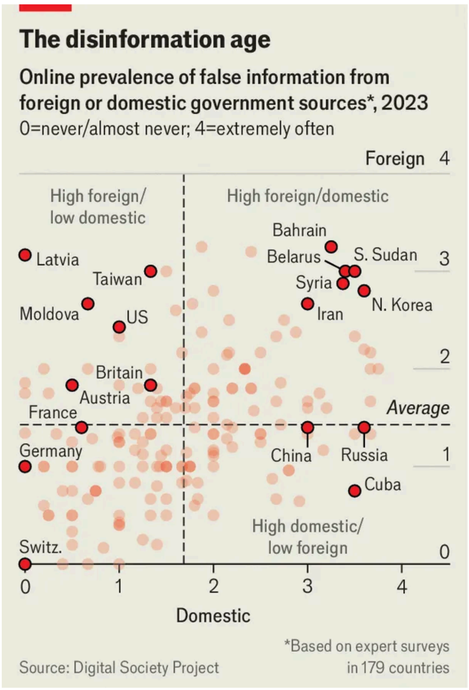

Figure 2. The mechanics of disinformation rise and spread. Adapted from "Disinformation is on the rise. How does it work?" by The Economist, 2024. Copyright 2024 by The Economist Newspaper Limited.

ACKNOWLEDGMENTS

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

- Aspen Institute Germany. (2024). *Hybrid Realities: Disinformation, Influencers, and the Defense of Democracy.*
- CBS Interactive. (2025, November 25). X's new feature reveals foreign origins of some popular U.S. political accounts. *CBS News.* https://www.cbsnews.com/news/x-foreign-origins-political-accounts/
- Council on Foreign Relations. (2012, August). Compromise of Saudi Aramco and RasGas. Council on Foreign Relations. https://www.cfr.org/cyber-operations/compromise-of-saudi-aramco-and-rasgas
- CSIS Issues Commentary: Demystifying Iranian Cyber Operations in the U.S.-Iran Conflict. (2026). In *Targeted News Service*. Targeted News Service.
- CSIS . (2025, December). Significant cyber incidents: Strategic technologies program. CSIS. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
- FBI. (n.d.). Russian interference in 2016 U.S. elections | Federal Bureau of Investigation. MOST WANTED. https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections
- iStock. (2025, February 20). [Photograph of digital disinformation]. In Disinformation is now part of mainstream politics. NordForsk. https://www.nordforsk.org/news/disinformation-now-part-mainstream-politics
- Nye, J. S., Jr. (2021). Soft power: The evolution of a concept. *Journal of Political Power, 14*(1), 196-208. https://doi.org/10.1080/2158379X.2021.1879572
- Retzmann, N. (2025). Narratives of Competition, Competition of Narratives? United States-China Relations, Technology, and the Role of Storytelling. *Global Studies Quarterly, 5*(2). https://doi.org/10.1093/isagsq/ksaf036
- Rid, T. (2021). *Active measures: the secret history of disinformation and political warfare* (First edition.). Farrar, Straus and Giroux.
- The Economist. (2024, May). Disinformation is on the rise. How does it work? [Graph]. The Economist. https://www.economist.com/briefing/2024/05/09/disinformation-is-on-the-rise-how-does-it-work
- Wilson, R., & Donnelly, N. (2026). Russia, Weaponized Social Media and Cyber Warfare: Ethical and Anticipated Ethical Issues. *International Conference on Cyber Warfare and Security,* 561-568.