NOT CYBERWAR, BUT CYBERBALANCE

DAVID BENSON

Most cyberattacks are not attempts to coerce or deterrence failures, but they are attempts to alter the balance of power. Extant IR theory accepts that states balance internally and externally by increasing domestic capacity and by partnering with other states, respectively. While balancing affects the balance of power by increasing power, states can also affect the balance of power by decreasing their competitors' power, or "handicapping." States wanting to handicap competitors can use certain kinds of information to decrease a competitor's capacity—information is important enough to economic and political processes but sufficiently removed from battlefield defeat to be less likely to provoke escalation. The internet's decreased costs and global scope have moved handicapping from the periphery of statecraft to a central position in international relations.

Theories of coercion, deterrence, and balance of power carry more explanatory power when considering cyberattacks that occur without readily apparent conflict sources. Questions of balance of power pervade the day-to-day machinations of international affairs, and such attacks, unaffiliated with a discernable war and often uncoercive in nature, are better understood as "handicapping." Handicapping aims to alter the balance of power by slowing political growth.

The Conundrum of Cyberattacks

In mid-January 2022, as tension between Russia and Ukraine escalated, Microsoft's cybersecurity units detected malware targeting Ukrainian computers.[1] How should strategists and planners have analyzed this malware? If the cyberattack heralded Russian tanks rolling across the border towards Kiev, military planners needed to act quickly to repel both the cyberattack and the invasion. Russia preceded invasions with cyberattacks in Georgia (2006) and Ukraine (2014), so anticipating invasion might seem

Dr. David Benson, assistant professor of security and strategic studies at the School of Advanced Air and Space Studies at Air University, specializes in the effects of information technology and international strategy, including cybersecurity and the internet.

1. Microsoft Threat Intelligence Center et al., "Destructive Malware Targeting Ukrainian Organizations," Microsoft Security Blog, January 16, 2022, https://www.microsoft.com/.

like a prudent maneuver.[2] But many Russian cyberattacks were not preludes to kinetic attacks, including cyberattacks on Estonia and the United States.[3] Responding to a cyber attack as if it is a military attack risks unnecessary escalation.[4] Not preparing for a war when one is imminent is imprudent.[5]

Many national and international security professionals, scholars, and commentators advocate for treating all cyberattacks as if they are the first blow of military attack. International relations (IR) scholars and foreign policy professionals struggle to understand and respond to cyberattacks, because we try to place them on the spectrum between war and peace. At least one philippic follows every transnational cyberattack calling the attack a "Cyber Pearl Harbor" or a "Cyber 9/11" and demands military retaliation.[6] Some even argue that by not treating cyberattacks like military attacks, we are functionally ceding a military domain to the enemy.[7]

Even if advocates for robust, military-like attitudes toward cyberattacks rarely propose military escalation, using verbiage generally reserved for military combat and war encourages misunderstanding and miscalculation. Focusing on the war/not war binary can lead observers to undervalue or overvalue cyberattacks by inappropriately equating them with categories that hide the attack's true effects.[8]

For those who ask whether all substantial cyberattacks are not equivalent to war, the question that must be answered is "if some important cyberattacks are *not* equivalent war, then what are they?" While it is an important first step to recognize that cyberattacks are "un-war," this only tells us what cyberattacks are not.[9] Given the risks of accidental escalation, why would a government allow something as provocative as the cyberattacks during the 2016 US presidential election? Knowing why such attacks happen will allow planners and policy makers to account and prepare for potential future attacks. Equally importantly, scholars and strategists can better develop counterstrategies by understanding what strategic objectives cyberattacks can pursue.

International relations theories of deterrence, coercion, and balance of power better explain many cyberattack campaigns occurring without obvious conflict sources.

---

2. Mark Clayton, "Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers," *Christian Science Monitor*, June 17, 2014, https://www.csmonitor.com/; and Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," *Security Dialogue* 43, no. 1 (2012).

3. Jim Finkle, "Agent.BTZ Spyware Hit Europe Hard after U.S. Military Attack: Security Firm," Reuters, March 12, 2014, https://www.reuters.com/; and Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (June 2011).

4. Robert Jervis, *Perception and Misperception in International Politics*, New Ed. (Princeton: Princeton University Press, 2017).

5. Randall L. Schweller, "Unanswered Threats: A Neoclassical Realist Theory of Underbalancing," *International Security* 29, no. 2 (2004).

6. See James J. Wirtz, "The Cyber Pearl Harbor Redux: Helpful Analogy or Cyber Hype?," *Intelligence and National Security* 33, no. 5 (2018).

7. Richard A. Clarke and Robert K. Knake, *The Fifth Domain* (New York: Penguin Publishing Group, 2019).

8. Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013).

9. Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017).

According to realist international relations theory, states (or more accurately their governments) jockey for advantage in the international balance of power.[10] Even IR paradigms that claim it is possible to mitigate balance-of-power concerns still accept the balance of power exists and *can* affect some governments' behaviors.[11] Balance of power can sometimes lead to conflict and war, but war is relatively infrequent compared to the pervasive concern over balance of power. Consequently, the phenomena comprising the daily grind of international politics are usually more concerned with the balance of power than with war.

Accordingly, many cyberattacks are attempts to revise the international balance of power—a phenomenon this article calls handicapping. Handicapping are attacks on a competitor that are attempts to revise the balance of power by slowing political growth. Handicapping as a concept rests upon the difference between the logic of coercion and the logic of balance. States may be coercing or balancing using either war or not-war, but coercion and balancing have orthogonal objectives.

Coercion exercises military power to resolve conflict in the state's interest *now*. Because coercion affects current political behavior, the logic of coercion uses (and affects) current power. Balancing develops economic and political power preparing to coerce, deter, or resist coercion *in the future*. Because the balance of power anticipates future conflict, the logic of the balance of power affects power development. Using power and developing power are conflicting objectives because typically, and as in war, using power consumes more resources than it creates.[12]

Making a theoretical distinction between handicapping attacks and coercive attacks opens potential policy options and makes opponent strategies clearer. Balance of power is not a new concept, but theorists and strategists refer to balancing as something a government does internally or by creating alliances.

Degrading competitors' capabilities to adjust the balance of power in your favor is logically consistent with the idea of a balance but nonetheless remains unexplored. When under a destructive attack, leaders do not want to be told, "We don't know what this is, but it is not war." Knowing that not only are many destructive attacks not trying to win a war now, but that those attacks are "handicapping" you for advantage in the future is an answer that illuminates strategies. If there really is time between a handicapping attack and a decisive point, the victim of the attack can pursue temporal strategies to deal with handicapping.

Distinguishing between attacks affecting the balance of power from coercive attacks sets standards allowing decision makers to assess whether escalation is appropriate. Attacks affecting the balance of power can happen any time and for any reason. By

10. Kenneth Neal Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979); and John J. Mearsheimer, *The Tragedy of Great Power Politics*, 1st ed. (New York: Norton, 2001).

11. Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton: Princeton University Press, 2005); and Alexander Wendt, *Social Theory of International Politics* (New York: Cambridge University Press, 1999).

12. James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995).

contrast, coercive attacks must happen either with clear communication of coercive intent or in a context where coercive intent is somewhat obvious.

Many of the most egregious cyberattacks over the past 10 years have occurred absent obvious coercive intent and without coercive messaging.[13] Leadership in the United States and elsewhere have frequently demurred from treating those attacks as war to the disappointment of some in the cybersecurity community.[14] But expending military power to meet a challenge meant to degrade power would have played into, not defeated, the attacker's strategy.

A Potential Instrument for Handicapping

One need not believe states always care about the balance of power to accept that some states sometimes care about the balance of power and behave accordingly. Rational concerns about the balance of power arise as states maneuver to improve their prospects of prevailing in future conflicts. Information is a vital component of power, so leaders caring about the balance of power can reasonably conclude that interfering with certain information might affect the balance of power. Information's character before the internet made many strategies that *could* affect the balance of power difficult. The internet changed the information topography, making strategies that plausibly affect the international balance of power possible and attractive.

States must care about the balance of power to hedge against future conflict. Interstate conflicts occur when one state attempts to coerce another. Conflict need not be military, but states can resist coercion as long as battlefield victory is possible, making military power and capacity important to balance-of-power concerns.[15] States resist coercion to retain their freedom of action. If coercion escalates to systemic war, the war can be catastrophic even for the victor, and the loser must accommodate itself to a disadvantageous international system.[16] Handicapping is a strategy that hedges against future coercion by impairing a competitor's ability to develop latent power or convert latent power into actual power.

Sources of Power

State power comes from many sources, but governments can only change some sources of power to swiftly affect the balance of power. For example, a 2005 RAND

13. Jason Chaffetz, Mark Meadows, and Will Hurd, *The OPM Data Breach: How the Government Jeopardized Our National Security for More Than a Generation*, Majority Staff Report, 114th Congress (Washington, DC: US House of Representatives, Committee on Oversight and Government Reform, September 7, 2016), https://republicans-oversight.house.gov/.

14. Mearshimer, *Great Power Politics*.

15. Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966); Robert Anthony Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996); and Daniel L. Byman and Matthew C. Waxman, *The Dynamics of Coercion* (New York: Cambridge University Press, 2002).

16. Robert Gilpin, *War and Change in World Politics* (New York: Cambridge University Press, 1981).

conference identified eight drivers of national power: domestic sociopolitical, international political, population, economic, agriculture, energy, technology, and environment.[17] Governments can affect all eight drivers of national power, but many—including population, energy, and environment—change only slowly, if at all.

Governments can more rapidly affect agriculture and technology, but while governments can easily harm existing agricultural and technological resources, developing such resources from nothing is harder. Therefore, governments must mostly rely on domestic sociopolitics, international politics, and economics to manipulate the balance of power.

The international mechanisms to create national power naturally attract substantial attention in international relations. Treaties are a source of international power and mechanisms for international competition as states jockey to ensure their interests become encoded in international agreements.[18] Joining organizations can allow states more power in international interactions than material power alone and can even set the terms of the international system.[19] Trade and economic exchanges are potential sources of material power and wealth, tools for competition, and mechanisms for cooperation.[20]

Domestic economic and sociopolitical power contribute directly to latent or potential power. Latent power includes the capability or resources to accomplish objectives but not the organizational mechanisms to pursue specific objectives. States with stable and unified political systems create an environment for robust economic growth.[21] Political stability can be a self-reinforcing cycle as increased instability decreases trust in government and political unity, thereby decreasing stability.[22] Domestic sociopolitical divisions make policy implementation more difficult and harm economic growth, whereas internal political stability makes government rent extraction easier.[23]

---

17. Gregory F. Treverton and Seth G. Jones, *Measuring National Power* (Santa Monica, CA: RAND Corporation, April 21, 2005), https://www.rand.org/.

18. Karolina M. Milewicz and Duncan Snidal, "Cooperation by Treaty: The Role of Multilateral Powers," *International Organization* 70, no. 4 (2016).

19. Christina J. Schneider, "Weak States and Institutionalized Bargaining Power in International Organizations," *International Studies Quarterly* 55, no. 2 (2011); and G. John Ikenberry, *Liberal Leviathan* (Princeton: Princeton University Press, 2012).

20. Stephen G. Brooks, *Producing Security: Multinational Corporations, Globalization, and the Changing Calculus of Conflict* (Princeton: Princeton University Press, 2005); Dale C. Copeland, *Economic Interdependence and War* (Princeton: Princeton University Press, 2014); and Patrick J. McDonald, *The Invisible Hand of Peace: Capitalism, the War Machine, and International Relations Theory* (New York: Cambridge University Press, 2009).

21. Kevin Grier, Shu Lin, and Haichun Ye, "Political Fractionalization and Delay in Fiscal Stabilizations: A Duration Analysis," *Public Choice* 164, no. 1/2 (2015).

22. Marc L. Hutchison and Kristin Johnson, "Capacity to Trust? Institutional Capacity, Conflict, and Political Trust in Africa, 2000-2005," *Journal of Peace Research* 48, no. 6 (2011).

23. Kjetil Bjorvatn and Mohammad Reza Farzanegan, "Resource Rents, Balance of Power, and Political Stability," *Journal of Peace Research* 52, no. 6 (2015).

The domestic sociopolitical system also enables actual power—the mechanisms to enact specific policies. In the realist tradition, actual power is sometimes used synonymously with military power, but in this article, actual power includes all government capacity to directly affect specific and immediate policies. Therefore, deploying the military to separate Panama from Columbia *and* building the Panama Canal both used actual power. Power use imposes economic costs on a state because capabilities and resources normally used to develop latent power are diverted to actual power: steel production is vital to both industry and the military, but every pound of steel used to make tanks cannot be used to make toasters.

Soft power merits special notice as a type of power because it merges domestic sociopolitical structure with international power without reliance on material power capabilities. A state's domestic economic strength creates material capabilities, which are a component of hard power, but soft power may change without underlying changes in capabilities. Soft power arises because another state's government or (more commonly) society is inherently attractive, has desirable social characteristics, or shares social ties with other states' populations. Soft power induces cooperation through social affinity.[24] Soft balancing is the conceptual antithesis of soft power, where governments resist a hegemon's power using nonmaterial means.[25]

Entire States Balance, Not Just Governments

Although the international balance of power is among states, governments are not the only actors in the international system who contribute to or benefit from favorable balances of power. The state is a useful theoretical fiction delineating bases of international power that different international actors can access. Governments have the most direct access to a state's power and are usually the most powerful international actors. Other actors contribute to and draw from a state's power, with or without the government's direction and support. Microsoft increases US power by developing the economy and consolidating rents from abroad. Microsoft also benefits from its position in the most powerful state in the world, being safe from external attack and with the US Government defending Microsoft's intellectual property.

Even in authoritarian regimes, nongovernment economic activity is tremendously important for the overall international political strength of the state. Companies and organizations contribute to or detract from political unity and stability depending upon their disposition toward and relationships with the government and each other. Private organizations affect economic growth as do financial markets. Companies and financial institutions constitute vital aspects of state power. Because civil society is an important part of a state, even self-interested civil society groups may affect state power. American automakers developed industry to compete with other countries'

24. Joseph S. Nye Jr., *Soft Power: The Means to Success in World Politics*, illustrated ed. (New York: PublicAffairs, 2005).

25. Robert A. Pape, "Soft Balancing against the United States," *International Security* 30, no. 1 (2005).

automakers, not for the glory of the government. Willys, Ford, and Chevrolet were still important components of American power in WWII.[26]

International actors contributing to and benefiting from a state's relative power position can also act to affect a state's relative power. Nongovernment entities can increase production, attempting to offset advantages other states have. Groups able to act internationally can also handicap competitors, fearing future advantages another state's relative power confers on the competing state. The actors responsible for balancing or handicapping do not change handicapping's and balancing's effects on the balance of power. When American economic power eclipsed the UK's economic power, driven as much by industrial development and private territorial expansion as any government policy, the relative importance of government policy versus private initiative did not change the outcome.[27]

Online the boundaries between government and civil society blur so far as to become almost indistinguishable. Many governments of all regime types directly employ cybersecurity professionals not directly responsible to the government. Sometimes relying on nongovernment actors is a strategy to obfuscate government involvement.[28]

Other times, civil society organizations pursue cybersecurity objectives on behalf of a state's citizens without guidance from the government and for their private purposes. For example, Microsoft has taken upon itself the task of improving cybersecurity as part of its mission.[29] Determining which actors are responsible for actions in specific circumstances remains important for policy but is less relevant to understanding overall state behavior. The balance of power changes no matter who makes the decisions.

Logic of Balancing vs. Logic of Coercion

Coercion is different from balancing because coercion addresses immediate, specific problems but balancing prepares for future problems. Because coercion is attempting to address immediate, discrete, and defined problems, coercion *must* deal directly with a government's ability to exercise actual power. While coercing governments may attack tools that develop latent power to inflict costs, if governments retain the ability to exercise actual power, they retain the ability to resist coercion.[30] Consequently, coercive attacks degrade the institutions, organizations, and resources that governments use to exercise power.

States balance by increasing their own ability to develop power by strengthening domestic sociopolitical institutions, building international relations, and fomenting

---

26. David Dalet, *The Jeep: History of a World War II Legend*, 1st ed. (Atglen, PA: Schiffer, 2013).

27. Nathan Rosenberg and L. E. Birdzell Jr., *How the West Grew Rich: The Economic Transformation of the Industrial World*, 1st ed. (New York: Basic Books, 1987).

28. Tim Maurer, "Cyber Proxies and Their Implications for Liberal Democracies," *Washington Quarterly* 41, no. 2 (April 2018).

29. Matt O'Brien, "Microsoft's Anti-Hacking Efforts Make It an Internet Cop," Associated Press, August 21, 2018, https://apnews.com/.

30. Pape, *Bombing to Win*.

economic growth. Balancing hedges against future needs to coerce, resist coercion, or deter when there is no immediate need to coerce. States do not need to use force now to want to hedge against security needs in an uncertain future.[31] Even relatively secure states able to relax in the short term might not want to fall so far behind other states—at some point a previously secure state may not be able to defend itself.

Handicapping—as with balancing—also hedges against future threats but does so by degrading a competitor's ability to develop power. Handicapping is offensive because it attacks the competitor, but the attack targets power development and occurs absent an immediate policy challenge. Degrading economic productivity and sociopolitical cohesion harms a competitor's ability to develop power. Handicapping intends to harm power development, whereas in coercion, harming power development is incidental to the attempt to coerce now. Handicapping by degrading a competitor's power-development capability *before* a crisis improves the likelihood the crisis will resolve in the handicapper's favor.

Examining edge examples like preventive and preemptive wars highlights the distinction between the logic of coercion and the logic of balance. In preemptive wars the attacker strikes an adversary when the adversary's attack is imminent. Preemptive wars follow the logic of coercion. The preemptor fears an immediate coercive threat and attacks first to countercoerce its adversary.

In preventive wars, a declining power attacks an ascending power in hopes of arresting the rising power's ascent. Preventive wars are closer to the logic of balancing but will usually still constitute attempts to coerce. Preventive wars historically have struck at the institutions and organizations established for actual power use, not at those with potential power creation, and are attempts to coerce the rising power into accepting secondary status.

For example, the US-led invasion of Iraq was a preventive war intended to stop Iraq's ability to develop nuclear weapons to increase its power. Some of the arguments for the Iraq war applied handicapping's logic—Saddam Hussein's relative power in the region must be reduced. During the war itself, however, the United States and its Allies and partners attempted to coerce Iraq first to accept UN inspectors, then to change governments.

Handicapping and coercion often look the same from the defender's viewpoint. It can be impossible to differentiate between handicapping and coercion using most instruments of power. Israel *may* have been handicapping Iraq by bombing the Osirak reactor, but that bombing looked exactly like an attempt to coerce Iraq into accepting Israel's military superiority.[32] The United States *might* have been attempting to slow Soviet economic growth with embargoes, but it looked to the Soviets exactly like

31. Evan Braden Montgomery, "Breaking out of the Security Dilemma: Realism, Reassurance, and the Problem of Uncertainty," *International Security* 31, no. 2 (2006); and Sebastian Rosato, "The Inscrutable Intentions of Great Powers," *International Security* 39, no. 3 (2015).

32. Richard K. Betts, "The Osirak Fallacy," *National Interest*, no. 83 (2006): 22–25.

America was attempting to use economic power to coerce the Soviets into changing domestic policy.

Attempting handicapping when the defender is likely to believe it is being coerced risks escalation. Governments acting aggressively can accidentally signal they are revisionist, provoking competitors to react accordingly and triggering a spiral of escalation.[33] Before the internet, most instruments of power were blunt and accidentally affected unintended targets, creating collateral damage the targets of the attack misinterpreted as the primary targets.[34] Even knowing the political organization, social structure, and economic institutions within a competitor's state with enough granularity to differentiate between actual power use and potential power development was outside the capacity of most governments before the internet.

Information and Power

As information technology develops, information—especially cheap, online information—is increasingly important to power creation and is easier to manipulate from a distance. Cyberattacks can use information to degrade a state's economic, political, and military power-creation capacities.

Economic

Information is crucial to creating latent economic power. Economic growth relies on innovation, which requires information.[35] A major source of economic growth is the development and dissemination of information allowing firms to recognize underserved market sectors.[36] Markets and market development are major engines of economic growth and are—at their core—information aggregation mechanisms.[37] Improved information technology and especially the internet dramatically increase economic development and latent power.[38]

Political

Information is also crucial to government operations. Governments require information to set and implement tax policies, extracting economic power to convert it to actual power. Information allows governments to coordinate efforts and make policy decisions. Governments and leaders share information as a matter of international

33. Jervis, *Perception and Misperception.*

34. Prashant Dikshit, *Precision Guided Munitions and Reduced Collateral Damage*, IPC S Issue Brief, no. 8 (New Delhi: Institute of Peace and Conflict Studies, May 2003), https://www.jstor.org/

35. Eric D. Beinhocker, *The Origin of Wealth: The Radical Remaking of Economics and What It Means for Business and Society* (Boston: Harvard Business Review Press, 2007).

36. Clayton M. Christensen, *The Innovator's Dilemma* (Boston: Harvard Business Review Press, 2016).

37. F. A. Hayek, "The Use of Knowledge in Society," *American Economic Review* 35, no. 4 (1945).

38. Jonathan L. Zittrain, "The Generative Internet," *Harvard Law Review* 119, no. 7 (2006).

statecraft.[39] Governments must accept international information, analyze it, and determine international policy. Misperception or miscalculation can be catastrophic.[40]

Military

Finally, information affects military power development and use. As militaries train, plan, and prepare for a potential war, sharing information within the military and with allies is necessary for military operations. In many instances, militaries must also guard against espionage during prewar preparations lest potential adversaries use compromised information to counter preparations. During war, there can be neither command nor control without information flow. Information is, therefore, among the most important commodities flowing through lines of communication.

Handicapping and Online Information

The importance of information in power generation makes handicapping possible. Competitors can chip away at latent power by slowing economic growth. Interfering with government operations can also slow latent power production, harm the conversion of latent power into actual power, and damage perceptions of power at home and abroad. Governments and civil societies use information to create a unified policy front either by aligning government policy with popular preferences or by coercing civil society into accepting government policy. Interfering with economic, government, and political processes and institutions slows a state's latent power creation.

Information has always been important, but before the internet, information's relative scarcity made attacking competitors' information difficult. Pre-internet information was closely held and difficult to obtain and manipulate. When governments attacked information, their strategies and operations were complex, costly, and tailor made. Cracking an opponent's cipher, seeding a political lie in an opponent's mass media, or stealing an opponent's secrets were major coups and could shift the overall balance of power. Such operations were also exorbitantly costly and so haphazardly successful as to preclude constituting a reliable strategy.[41] Governments tried, of course, but were so infrequently successful that scholars and policy makers could afford to outsource concern about information to persons involved in information operations per se.[42]

Effectively using information to harm a competitor's international power requires information about the competitor's domestic political environment. Overseas competitors can collect and analyze mass online data (data analytics) almost as easily as

39. John J. Mearsheimer, *Why Leaders Lie: The Truth about Lying in International Politics* (Oxford: Oxford University Press, 2013).

40. Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY: Cornell University Press, 2010).

41. Lindsey A. O'Rourke, *Covert Regime Change: America's Secret Cold War* (Ithaca, NY: Cornell University Press, 2021).

42. O'Rourke, *Covert Regime Change*.

domestic groups. The inability to understand domestic political situations hindered pre-internet attempts at informational handicapping.[43] For example, Soviet misunderstandings about the US Civil Rights movement effectively precluded their exploitation of domestic discontent weaken the United States at home.[44] Online information makes understanding competitors' domestic sociopolitical terrain easier. Russian information operations in 2016 identified and exploited salient divides within the electorate.

Competitors can also use deception and computer security vulnerability exploitation to collect information that itself is useful in handicapping. Phishing is a sophisticated version of deception, presenting victims with inauthentic versions of websites to steal security credentials, but deception could be as simple as lying about identities on social media.[45] Overseas actors using extant computer security vulnerabilities can access valuable information by exploiting weaknesses in code or using malware to introduce vulnerabilities to systems to steal privileged information.[46] The internet makes in-person theft more effective because agents' digital storage media store so much more information.

The internet makes information injection in domestic information environments easier. In 1960, most countries had at most a few national newspapers and television or radio networks, but now every outlet potentially spans the globe. Even if getting a story printed in your competitors' domestic media is no easier now than 50 years ago, the proliferation of national outlets increases potential injection points. Social media's global reach allows international actors to draw attention to native media coverage, exploiting social media algorithms to ensure stories they support see increased attention.[47] Most social media platforms offer targeted advertising, essentially allowing adversary governments to outsource their information operations to domestic actors in the target state.

Potential Handicappers

Governments may actively or passively employ a handicapping strategy online. When governments *actively* handicap adversaries online, government entities attack competing states' power-creation capabilities using cyberattacks. Governments may also passively follow a handicapping strategy by tolerating attacks against competitors'

43. Arch Puddington, *Broadcasting Freedom: The Cold War Triumph of Radio Free Europe and Radio Liberty* (Lexington: University Press of Kentucky, 2000).

44. Christopher Andrew and Dmitri Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999), 236–39.

45. See Cedric Pernet and Eyal Sela, "The Spy Kittens Are Back: Rocket Kitten 2," research paper (Irving, TX: Trend Micro, September 1, 2015), https://documents.trendmicro.com/.

46. See Crowdstrike Global Intelligence Team, *Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units* (Austin, TX: CrowdStrike, December 22, 2016).

47. Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* 11, no. 4 (November 2017).

power creation. Tolerating attacks against competitors' power allows a government to deny responsibility for attacks while reaping the competitive benefits.

When states tacitly allow online attacks against competitors' interests, the attackers' immediate goals may not entail the international balance of power but affect the balance nonetheless. The ransomware gangs Russia tolerates (as long as they do not attack Russian targets explicitly) argue their interests are nonpolitical.[48] Insofar as ransomware and other forms of cyberattacks can be lucrative, we need not impute motives absent evidence to explain why such criminal organizations would emerge. Since governments and their domestic civil society groups operate in similar circumstances, interest alignment should not be surprising. If a government controls a state with less relative power than a competitor, the competitor is also usually more wealthy. Wealthy states possess many lucrative targets for criminals.

Entities within states targeted by handicapping also respond absent government impetus for their own reasons. Companies targeted by cyberattacks do not need a government to tell them losing money is bad, and they will respond accordingly. Both the need to secure their own corporate information and the opportunity to make money securing other companies' information drives these organizations to develop cybersecurity defense capabilities. Microsoft, FireEye, or CrowdStrike have sufficient profit motive to counter cyberattacks that they will act independently of the government.

The Nature of Handicapping

Many recent cyberattacks make more sense when thought of as attempts to affect the balance of power. The United States and its allies compete with Russia and China, but there has been no specific conflict and few of the crises that defined the Cold War. Nonetheless, Russia and China have supported or allowed massive cybercampaigns attacking institutions and organizations contributing to national power, including corporations, financial institutions, government organizations, and political institutions. Cyberattacks leach away billions of dollars in direct costs while diverting other resources.[49]

Russian cyberattacks on the United States drew the government's competence into question, potentially destabilizing alliances and governing coalitions, and cost the US economy billions of dollars. In 2009, the Russian worm agent[.]btz infiltrated the NIPR military network in the Middle East and stole military information; Operation Titan Rain expunged a Chinese worm attacking US military networks in 2005; and in the months leading up to the 2016 US presidential election, Russian hackers penetrated the computers of the Democratic National Committee and the Democratic

48. Graham Cluley, "The DarkSide Ransomware Gang Must Be Shitting Itself Right Now," Graham Cluley (blog), May 11, 2021, https://grahamcluley.com/.

49. Phil Goldstein, "Cybersecurity Funding Would Jump in Trump's 2019 Budget," *FedTech*, February 2018, https://fedtechmagazine.com.

Congressional Campaign Committee.[50] None of these attacks occurred within the context of ongoing conflicts, but each attacked a component of American power, plausibly harming America's position in the international balance of power.

Attacks on political institutions may have the greatest but most difficult to assess effect on political power. Russian interference in the 2016 election dominates both research and commentary explaining transnational interference attacking political institutions. Russian cyberattacks against electoral institutions in 2016 actually began in 2014—Russian hackers stole information from a wide variety of electoral targets for a span of two years.[51] And although it remains unclear if the hacks changed the outcome of the election, Russian cyberattacks contributed to decline in perceived legitimacy of American elections.[52]

Handicapping Is Competition, Attacking Is Conflict

Military strategy and international politics must grapple with the challenges of competition among great powers while avoiding conflict. Competition in a world of nuclear weapons may be dangerous, but it is unavoidable. In cyberspace and in the real world, China, Russia, and others *compete* with the US and its allies for preeminence in the international system. In international competition, competing governments pursue their own interests. For example, the United States does not want an international system where governments can militarily realign borders. Russia wants to control parts of Ukraine with its military. Even before Russia invaded Ukraine, it was competing with the United States to achieve its aim.

Conflict is destructive and dangerous. In the nuclear era, conflict may escalate to nuclear exchange. Once citizens start dying, nuclear-armed governments may retaliate with nuclear weapons. In fact, nuclear deterrent strategies like establishing "tripwires" specifically rely on the possibility that deaths may lead to escalation.[53] Governments take even the potential for nuclear exchange seriously and change their behaviors

50. Anton Cherepanov and Robert Lipovsky, "New TeleBots Backdoor Links Industroyer to NotPetya for First Time," WeLiveSecurity, October 2018, https://www.welivesecurity.com/; Department of Justice (DOJ) Office of Public Affairs, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace" (Washington, DC: DOJ, October 19, 2020), https://www.justice.gov/; David Alexander, "Pentagon Flash Drive Ban Has Many Exceptions," Reuters, June 2013, https://www.reuters.com/; and Raphael Satter, Jeff Donn, and Chad Day, "Inside Story: How Russians Hacked the Democrats' Emails," Associated Press, November 4, 2017, https://www.apnews.com/.

51. Public Broadcasting Service (PBS) Newshour, "Reconstructing the Russian Hacks Leading up to the Election," PBS, December 14, 2016, https://www.pbs.org/.

52. Shaun Ratcliffe and Simon Jackman, "State of the United States Poll: Free and Fair? American Attitudes towards Electoral Integrity and Legitimacy" (Sydney, Australia: United States Studies Centre, November 3, 2020), https://www.ussc.edu.au/.

53. Schelling, *Arms and Influence*.

accordingly.[54] Despite the possibility of nuclear weapons use, conflict has erupted from time to time, sometimes even between nuclear-armed countries.

Competition is part of normal politics, but conflict is war. No two governments, not even Allies, have a perfect harmony of interests. Even the United States and the United Kingdom—a treaty ally—competed with each other in pursuit of their own interests. Competition over fishing rights in the North Atlantic almost exclusively involved NATO allies. During the Cold War, the United States and the Soviet Union openly competed across many venues but never openly fought one another. Both governments were aware that once conflict broke out, neither government would like the ultimate outcome.

Differentiating between competitive handicapping and coercive war in strategy and lexicon reduces the risks of accidental escalation. Had the United States responded to the revelation that Russian hackers had infiltrated the SolarWinds supply chain like it would if Russia had been flying bombers in US airspace, the consequences could have been catastrophic.[55] Even using such language risks miscommunicating national intent to partners, competitors, and even subordinates who might act as if war is imminent. A shifting balance of power is at least as important as being coerced, but it is not imminent. Using the language of balance of power conveys the grave situation without the added immediacy that can lead to rash decisions.

Knowing some cyberattacks are part of a long-term strategy rather than a short–term coercive burst opens a world of potential responses unavailable when resisting coercion. Because coercion is immediate, the only options available are to either accede to coercive demands or use the tools you have available at that moment. Dealing with shifting balances of power allows policies and strategies that take more time. Governments can counterhandicap, of course, but outbound handicapping need not take the same form as inbound handicapping.

States may simply attempt to outgrow the effects of handicapping rather than respond to it directly, compensating for any reduced power by replacing it with more power. Hardening institutions and systems against cyberattacks is an appropriate response to both handicapping and coercion, but these actions are more valuable when dealing with balance-of-power concerns. Handicapping may happen any time, so hardening against it pays off all the time.

Conclusion

Handicapping in international relations explains one of the more inscrutable online state behaviors—rampant transnational attacks absent coercive or deterrent issues. States, long concerned with their relative power, continue to compete online as they have in the real world. Russia developed offensive cybersecurity capabilities to handicap

54. Vipin Narang, *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict* (Princeton, NJ: Princeton University Press, 2014).

55. Molly Crane-Newman, "Russia Could Cut Off U.S. Food and Water Supply in Next Cyberattack, Romney Says," *NY Daily News*, December 20, 2020, https://www.nydailynews.com/.

the United States and its alliance structure to shift the balance of power in its favor. We now know for certain that humbling Ukraine has long been among Russia's goals.

The polemical rhetoric sometimes applied to energize political leaders and members of society to take cybersecurity seriously is misdirected but not wrong. Cyberattacks are a serious problem and cybersecurity is a major venue for international competition, but not all cyberattacks are acute problems with immediate solutions. International competitors recognize the potential to use online information to affect adversary national power and act accordingly.

Declining relative power is in many way a more severe problem than merely being coerced. Governments at a disadvantage in the balance of power are subject to repeated adverse coercion, not just the single incident in question. Alarming rhetoric missteps by equating immediate events that will matter now with the long, slow march of international strategy.

Handicapping also shows cyberattacks are more important than sometimes argued because they are an issue of international statecraft. Failure to treat cyberattacks with appropriate gravity risks underbalancing. Scholars and observers outside information security and cybersecurity circles are sometimes skeptical of cyberattacks' importance, because they rightly perceive their immediate effects as limited.

No cyberattack so far is as immediately physically destructive as a single joint direct attack munition (JDAM), but handicapping cyberattacks can have effects with longer-term consequences than the physical destruction bombs create. Indeed, handicapping cannot be as destructive as a JDAM, because such destruction almost assuredly provokes escalation and retaliation. Transnational cyberattacks are therefore less akin to one runner drugging the other to win a single race than they are to the same athlete altering another's diet to induce diabetes and removing the competitor as a challenge altogether. Acute problems may be frightening, but chronic problems are often far worse.

Handicapping also creates a useful frame for understanding the national security interest in issues like Huawei's involvement in 5G or information collected by companies under Russian or Chinese government influence. It is improbable companies like Huawei or Bytedance could acquire actionable intelligence relevant for military operations, or helpful in coercing democracies, while scraping random user data. This article shows how companies under a government's control could collect information deleterious to democratic and free-market institutions.

TikTok and Chinese telecoms are collecting the same kind of information Walmart wanted to collect on TikTok's American users and that SolarWinds collects from its customers. China and Russia are now using the information collected by TikTok and Chinese telecoms to handicap.[56] Assurances that information is secure ring hollow when the people who control access live under authoritarian regimes. In 2020, three

56. Joseph Pisani and Tali Arbel, "What Does Walmart See in Tiktok?," TechExplore, August 30, 2020, https://techxplore.com/; and Stephanie Kirchgaessner, "Revealed: China Suspected of Spying on Americans via Caribbean Phone Networks," *Guardian*, December 15, 2020, https://www.theguardian.com/.

miscreants used nothing more than a telephone to trick Twitter employees into surrendering access to some of the highest-profile Twitter accounts in the world.[57]

When Russia positioned forces along the Ukrainian border during an international political crisis, leaders had good reason to think early attacks were coercive and should have treated the attacks as a preparation for war. Russia did eventually invade Ukraine, and the only thing the Ukrainians could do was resist coercion. Fortunately, there are more options to respond to handicapping than merely resisting, and the United States and its allies retain those options in the face of Russian handicapping. Regardless of how the war in Ukraine ends, international competition and handicapping will continue. If the United States preserves its position in the balance of power using the many resisting strategies available, Russia and other revisionist states' handicapping will fail. ***Æ***

57. Catalin Cimpanu, "How the FBI Tracked down the Twitter Hackers," ZDNet, August 1, 2020, https://www.zdnet.com/.