

Great Power Cyberpolitics and Global Cyberhegemony

Yavuz Akdağ

As interstate cyberconflict intensifies, the intersection of national security, cybersecurity, and International Relations (IR) theory has emerged as a critical venue for scholarly inquiry. Yet due mainly to epistemological problems, IR theory has been limited in examining how it informs the maximization of strategic cyberpower and in testing key realist concepts and assumptions against cyberactualities, risking theoretical stagnation and conceptual infertility in the study of statecraft and cybersecurity. I seek to bridge these theory-testing and conceptual gaps by assessing offensive realism's assumption about the scope of hegemonic expansion in cyberspace using the crucial case of the United States. I argue that offensive realism has meaningful explanatory and predictive power in cyberspace but sometimes lacks this power under conditions assumed by the theory, emphasizing the need to modify offensive realism's understanding and scope conditions of hegemony. The US pursues global, not regional, cyberhegemony using offensive strategies to maximize its cyberpower for cybersecurity. Therefore, I critically examine defensive realism and cyber persistence theory as alternative structural perspectives on the pursuit of security in cyberspace and introduce a modified conceptual framework for hegemony to adapt offensive realism to cyber-realities. This conceptual innovation can potentially contribute to policy making and help to build a cyber-specific version of offensive realism.


Keywords: Global cyberhegemony, hegemonic cyberconflict, cyberpower, offensive realism, defensive realism, cyber persistence theory

Cyberspace has unveiled a new domain for power politics, one in which states increasingly engage in cyberconflict to achieve strategic ends by exploiting the growing global interconnectivity of the internet and the vulnerabilities it contains. In 2007 and 2008, Russia orchestrated cyberattacks on key Estonian and Georgian services to influence the political decision making of these countries. In 2010, experts discovered “Stuxnet,” a cyberweapon made by the United States and Israel, which damaged many centrifuges in an Iranian nuclear facility with

the goal of taming Iran's nuclear ambitions (Farwell and Rohozinski 2011, 26–30; Russell 2014, 4). In 2015, Russia targeted Ukrainian power grids amid the geopolitical conflict over Crimea and meddled in the US presidential election the following year. These incidents suggest interstate cyberconflict has intensified over the last two decades (Nye 2017, 48–49; Park and Walstrom 2017).

The peculiarities of cyberspace offer actors opportunities and incentives for cyberconflict as an attractive alternative to conventional warfare. Cyberconflict can be executed with legal impunity, and can provide the instigator with deniability, anonymity, and arguably more leverage over conventionally weaker players. It is less escalatory than conventional warfare, cost effective, relatively accessible due to low entry barriers, and free from temporal and spatial constraints, allowing continuous contact between actors. These elements are a function of the secrecy of cybercapabilities, perceived offense dominance, and the lack of regulatory frameworks for cyberspace, making cyberconflict an enticing strategic option for states (Choucri 2012, 11; Craig and Valeriano 2016, 141–44; Harknett and Smeets 2022, 543–44; Healey and Jervis 2020, 34–35).

Cyberconflict and cybercompetition enable nations to shift the global, regional, or bilateral balance of power

Yavuz Akdağ  (yavuzakdag@hakkari.edu.tr or akdaglar20@hotmail.com, Turkey) is an assistant professor in the Department of Political Science and International Relations at Hakkari University. He earned his PhD in Politics and International Affairs from the University of South Florida (USF) in 2023, focusing on the intersection of national security, cybersecurity, and international relations theory. Akdağ also holds a master's degree in Political Science from USF (2017) and a bachelor's degree in International Relations from Selçuk University (2012). His research explores international relations theory, international security, and great power cyberpolitics and cybersecurity.

doi:10.1017/S1537592725000040

© The Author(s), 2025. Published by Cambridge University Press on behalf of American Political Science Association. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

without conventional escalation.¹ A state actor, for example, can steal sensitive data on its adversary's military technology (e.g., missile plans), potentially causing the rival to lose its technological advantages and changing a symmetric power relation into an asymmetric one (Choucri and Clark 2018, 14; Harknett and Smeets 2022, 535–43). China's attempts to steal data on the US's F-35 Joint Strike Fighter is arguably aimed at accelerating its own military development while eroding American technological superiority, potentially shifting the distribution of power in Beijing's favor (Fischerkeller and Harknett 2019, 267–76).

Acknowledging the impact of cyberconflict and cybercompetition on power dynamics, great powers have officially treated cyberspace as a domain of warfare and accelerated cybermilitarization (US Department of Defense 2011, 5–7). The US, for example, established Cyber Command in 2010 and set out to compete in cyberspace by adopting the offensive cyberstrategies of “persistent engagement” and “defend forward” in response to increasing perceived cyberthreats (US Department of Defense 2018).

Because growing cybercompetition significantly threatens national security, the intersection of cyberthreat, national security, and IR theory has emerged as a crucial venue for scholarly inquiry (Clarke and Knake 2010; Nye 2017, 45). Several realist theoretical frameworks have informed the intricate dynamics of state-to-state cybersecurity relations over the last few decades (Choucri 2012; Gartzke and Lindsay 2015, 316; Saltzman 2013). For example, scholars have invoked fundamental Cold War nuclear deterrence principles to construct cyberdeterrence strategies for cybersecurity (Libicki 2009; Nye 2017).

Yet realist IR theory has either been slow or limited in treating cyberconflict as a complex, multifaceted aspect of great power cyberpolitics (i.e., in addressing how realism informs the maximization of strategic cyberpower), and in testing key realist concepts or assumptions against cyberrealities (Buchanan 2016, 9; Choucri and Clark 2018, 289; Whyte and Mazanec 2023, 46–49). Most studies lack systematicity, rigor, empirical robustness, and conceptual innovation (Gorwa and Smeets 2019, 2; Whyte and Mazanec 2018, 47; 2023, 46). For instance, cyberdeterrence intellectually derived from a defensive realist balance-of-power perspective is significantly challenged by the opaque nature of cyberpower, prompting analytical barrenness and a mismatch between theory and reality in the study of cyberdeterrence within IR theory (Taddeo 2018, 341; Waltz 1981).

Other studies have tested IR concepts and assumptions to inform cybersecurity issues such as the offense-defense balance (Saltzman 2013, 41; Slayton 2017, 74; Valeriano, Jensen, and Maness 2018). However, theory testing has remained marginal mainly due to epistemological problems. The characteristics of cyberconflict (e.g., the

confidentiality of cyberoperations) render most digital actions concealable, and thus data collection and knowledge accumulation are intractably challenging. Consequently, establishing a connection between actors' cyberactions and underlying motives becomes problematic, making theory testing difficult (Whyte 2018, 521–31).

Applying *untested* IR concepts and assumptions to cyberspace risks theoretical stagnation, as reflected in the poor explanatory schemes in, and diminished conceptual productivity of, the study of cyberdeterrence within IR scholarship (Kello 2013, 12; Whyte and Mazanec 2023, 46). This has raised skepticism about the relevance of realist IR theory to cyberspace and diverted focus to the new strategies of “persistent engagement” and “defend forward” to counter cyberthreats. Cyber persistence theory (CPT) underpins these strategies, representing a radical shift away from the IR-informed security paradigm and its associated concepts, such as coercion. This can hinder novel analytical attempts to understand the unique characteristics of cyberdynamics from an IR perspective, which may lead to faulty policy (Fischerkeller, Goldman, and Harknett 2022; Soesanto and Smeets 2021, 394).

The rise of cyberconflict calls for adjustments or unique approaches within IR theory, but not a radical break from existing theories or concepts in the absence of empirical testing and adaptation to the particular characteristics of cyberspace. Historically, revolutionary technologies (e.g., atomic bombs) have stimulated scholarly efforts to test established theories and assumptions against the new realities the technologies create (Brantly 2018, 32; Choucri and Clark 2018, 362; Kello 2013; Rid 2012, 351; Whyte and Mazanec 2023, 46). As one such revolutionary technology, cyberspace persists as a theoretical and practical challenge because IR theory mostly remains untested in this new domain (Choucri and Clark 2018, 362; Tor 2017, 92–111; Whyte and Mazanec 2023, 46).

I confront this challenge by bridging theory-testing and conceptual gaps in the study of cyberconflict, great power cyberpolitics, and IR theory. I test the empirical relevance of offensive realism (OR) by examining how well its assumption of hegemonic power maximization—the idea that regional hegemons would seek global expansion of their power if natural barriers (e.g., oceans) were removed—holds in cyberspace. I use the US as a case study because of its close relation to the theory.² I analyze major US cyberpolicies and cyberstrategies from 2003 to 2023, including the cases of Stuxnet in 2010 and the Snowden revelations in 2013. If the implications of OR's assumption about the scope of hegemonic expansion are correct, then Washington can be expected to expand its cyberpower and influence beyond its hinterland to achieve *global cyberhegemony*, as the borderless nature of cyberspace removes the strategic hurdles to global power projection.³

I argue that OR still has meaningful inferential and predictive power in cyberspace, though this is not always so under the conditions assumed by the theory. Thus, I emphasize the need to amend the theory's scope conditions for hegemony and propose an alternative conceptual framework regarding hegemony. This innovative approach can contribute to building a cyber version of OR and offer policy prescriptions that will enable great powers to optimize their cybersecurity.

In the remainder of the article, I will first define basic but controversial concepts such as cyberspace and cyberpower, and underline the need to align IR theory with the new cyber-realities. I also briefly discuss CPT, a structural understanding of cyberspace that offers a competing perspective on global cyberhegemony as a structure-driven outcome, allowing me to compare its strategic logic and policy prescriptions with the modified form of OR, which posits that states will expand their power endlessly in the absence of physical constraints. Second, I provide theoretical frameworks by comparing OR to its primary alternative, defensive realism (DR); I reconceptualize OR's understanding of hegemony to adjust the theory to cyberspace. Next, I test the empirical relevance of OR's assumption about the limits of hegemonic expansion in cyberspace, and conclude with significant theoretical and policy implications.

Cyberspace

In recent decades, technological advances driven by scientific breakthroughs have opened a new venue for human interaction: cyberspace (Choucri 2012, 6). The prefix "cyber" encompasses "a variety of digital, wireless, and computer-related activities" (Nye 2017, 46). The term "space" means "domains of interactions" that have their own resources, power sources, and actors seeking to increase their leverage. While IR theory focuses on interstate relations conforming with the notion of "territoriality," cyberspace emphasizes nonterritoriality (Choucri 2012, 5–6).

As a nascent domain, the study of cyberspace is marked by conceptual diversity (Lindsay 2017, 494). While cyberspace can structurally be divided into four layers (e.g., physical and informational layers), many of these layers are only concerned with its technical architecture and thus are not very relevant to IR scholars, who are fundamentally interested in how cyberactors use this domain to pursue power and strategic interests. This is important because cyberinsecurities emerge due to the combination of the structural design of cyberspace and the activities, interests, and motives of actors (Choucri and Clark 2018, 39–52). Therefore, I define cyberspace as a global, operational, political, and man-made domain where human interactions are enabled by interconnected computing devices to create, store, exchange, modify, and exploit electronic information, and to facilitate communication between users (Akdağ 2017, 102; Choucri and Clark 2018, 33; Nye 2011, 122).

Unlike natural domains, cyberspace requires human maintenance (e.g., installing fiber-optic cables) to function. Cyberspace is technologically malleable and replicable: as one platform is destroyed, another can be opened swiftly. As a global venue unconfined by geography, cyberspace has shifted the dynamics of geopolitics and shaped states' foreign policies. While cyberspace has physical, border-traversing components that subject it to some restrictions (e.g., governmental regulations), geographical constraints are dramatically removed in the new domain. Its interconnectedness enables instant and persistent contact, which lowers the costs of transportation and deploying force in this sphere (Harknett and Smeets 2022, 544; Zook, Devriendt, and Dodge 2011, 94). The nongeographical property of the domain allows worldwide participation, as entering cyberspace requires only a computing device and an internet connection, making it easily accessible and participation cost effective (Choucri 2012, 4; Harknett and Smeets 2022, 543–44; Sheldon 2011, 96–98).

Cyberspace is "structured" by interconnectedness, not by the "segmentation" characteristic of "episodic," "potential," or "imminent" state-to-state territorial contact (Fischerkeller, Goldman, and Harknett 2022, 30–31). This interconnectivity creates continuous contact among states, potentially affecting national power dynamics. This "constant contact" is a structurally imposed "condition" (Fischerkeller and Harknett 2019, 274), substituting the traditional understanding of temporality with the "near instantaneity" of cyberinteractions (Choucri 2012, 4).

CPT treats interconnectivity, reconfigurability, and continuous contact in cyberspace as key structural features critical to understanding how states pursue cybersecurity and national interests. These features create a "cyber strategic environment" where security is scarce, and where states are structurally incentivized to persistently seize and maintain the initiative to (re)establish favorable security conditions in and through cyberspace (Fischerkeller, Goldman, and Harknett 2022, 24). Initiative persistence can maintain or alter the interstate balance of power through cumulative strategic effects generated by exploitative actions over time. For CPT, the cyberenvironment is noncoercive because it favors exploitation as the dominant behavior and the "primary route towards gain" (Fischerkeller, Goldman, and Harknett 2022, 7). "Cyber faits accomplis" (internal balancing) and "direct cyber engagement" (external balancing) are key behaviors states manifest to exploit vulnerabilities and opportunities. This prompts "agreed competition" wherein "competitive interaction" that is "inclusive of operational restraint" and "exclusive of operations" short of armed-conflict equivalence emerges as the dominant dynamic in cyberspace (Fischerkeller, Goldman, and Harknett 2022, 50–59).

While CPT and modified OR draw distinct implications and prescriptions from the structural features of cyberspace (e.g., the logic of exploitation versus the logic

of expansion), to which I will return, both converge on the strategic saliency of the domain. Cyberspace presents states with sufficient incentives and opportunities to gain strategic advantages over adversaries, potentially shifting the balance of power. This has made cyberspace an arena for power politics and competition across two dimensions: (1) the management of cyberspace; and (2) cybersecurity (Brandes 2013, 90–93; Choucri 2012, 4–9; Ebert and Maurer 2013, 1058–64; US Department of Defense 2018). The clash over governance reflects a tension between the US-sponsored multistakeholder model, which promotes an open and decentralized management of the internet, and the multilateral model supported by authoritarian regimes (e.g., China), which demands more control over the internet (Gao 2022, 15–16; Hill 2014, 26–30). The cybersecurity dimension concerns competition between great powers to revise the cyber status quo by reallocating resources, shifting security dynamics, and amending governing rules (Ebert and Maurer 2013, 1054–58). Cybersecurity is most fundamentally concerned with the ability of a state to protect its cyber and kinetic components (e.g., its servers and economy) from threats (Choucri and Clark 2018, 139). Cybersecurity competition mostly involves economic espionage, intelligence gathering, digital sovereignty, and the militarization of cyberspace (Harold, Libicki, and Cevallos 2016, 9). When states struggle for cybersecurity or cyberpower, politics naturally ensues (Choucri 2012, 4–9).

Cyberpolitics

While the global and operational characteristics of cyberspace are well recognized, its political saliency has been overlooked. It is an arena wherein states negotiate, bargain, contend, compete, and engage in conflict over resources or institutional processes—the fundamentals of power competition. This fact, coupled with the growing awareness of cyberthreats, the involvement of multiple actors, attribution problems, and perceived offense dominance, has elevated cyberissues to high politics, which is closely linked to national security matters (Choucri 2012, 4–9; Ebert and Maurer 2013, 1054–56; Limnéll 2017, 42–43).

Yet cyberpolitics lacks a precise definition due to its infancy. It can be conceptualized as a process of politics driven by human interactions to authoritatively determine “*who gets what, when, and how*” in cyberspace—a new contested domain with its own methods and procedures. In cyberpolitics, actors struggle to influence or control resources and the behavior of others. For example, a state’s cyberdeterrence engagements involve cyberpolitics because they seek to shape an opponent’s payoff calculation within cyberspace. Because politics implies some degree of struggle, actors’ relative cyberpower is the essential determinant of their political interactions in cyberspace (Choucri 2012,

4–9; see also Caveltly 2018, 304; Limnéll 2017, 42–43; Valeriano and Maness 2017, 261).

Cyberpower

Notwithstanding its growing importance, the concept of cyberpower remains undertheorized in realist IR scholarship, with most analyses limited to US strategy and policy (Caveltly 2018, 305). Nevertheless, the literature offers workable definitions of cyberpower. Some scholars conceptualize it as “the ability to apply typical forms of control and domination in cyberspace” (Valeriano and Maness 2017, 261–66).

Other studies have addressed the multidimensional aspects of cyberpower using various conceptual, theoretical, and normative perspectives to establish a structured analysis. Joseph Nye (2011, 123) defines cyberpower as “the ability to obtain preferred outcomes through use of electronically interconnected information resources of the cyber [domain].” Nye also describes three different manifestations of cyberpower—restrictive cyberpower, deterrent cyberpower, and compellence. Restrictive cyberpower leaves limited choices for adversaries via defensive means (e.g., firewalls), whereas deterrent cyberpower seeks to mold actors’ preferences to avoid harmful actions (e.g., using retaliatory threats to deter). Compellence, however, aims to force adversaries to do something against their will. The purpose of Stuxnet, for example, was to make Iran concede to the US’s will (Nye 2011, 122–32; Valeriano, Jensen, and Maness 2018, 106). John Sheldon (2011, 96–97) defines cyberpower as “the sum of strategic effects generated by cyberoperations in and from cyberspace.” The purpose is to gain advantages over adversaries, reduce their capacity to understand the strategic environment, and achieve foreign policy objectives.

David Betz and Tim Stevens (2011, 145–53) offer an alternative conceptual framework that identifies four dimensions of cyberpower, challenging Nye’s direct, centralized, coercive form of power relations with their focus on indirect and more diffused institutional, structural, and productive forms of cyberpower. While these typologies exhibit “forms of dominations to the exclusion of ‘power to,’” Alexander Klimburg’s (2011, 43–44) Integrated Capability Model stresses the importance of the nexus between cybersecurity and cyberpower. A country’s cyberpower is also measured by its ability to defend itself against cyberthreats and achieve security in cyberspace (Caveltly 2018, 309–10). Frameworks that take defensive capabilities into account paint a more accurate picture of the interstate balance of cyberpower and reveal a paradoxical situation in which nations with the greatest cyberoffensive power are often the most vulnerable (Valeriano and Maness 2015, 25).

As the discussion above indicates, cyberpower is imprecise, multifaceted, and heterogeneous. Its definition varies depending on the theoretical lenses with which one seeks

to understand and explain the nature of power relations in cyberspace. Liberal IR theory ties cyberpower to institutional mediation, but liberal institutions are either nonexistent or underdeveloped in this sphere (Craig and Valeriano 2018, 88; Keohane 2020, 2–6). Constructivist and poststructuralist theories of IR challenge conventional explanations of the nature of power in cyberspace. Instead they highlight different sources of power such as productive power, yet cyberpower produced through language and social interactions between states and between state and nonstate entities is harder to quantify due to its indirect and diffused nature.

A realist explanation of cyberpower, as reflected in Nye's model centered on coercive power, remains the most viable conceptual tool to use, given its relatively measurable and attributable characteristics (Cavelty 2018, 308–16). Nevertheless, accurately assessing both a state's cyberpower and the interstate balance of power in cyberspace remains challenging due to cyberpower's stealthy characteristics and its ubiquity—that is, its ability to exert an effect across multiple domains beyond cyberspace (Sheldon 2011, 99–100; see also Valeriano and Maness 2017, 266).

However, not all scholars believe that cyberpower can be coercive, a discussion I will return to below. Nevertheless, many concur that cyberpower is a relatively flexible and useful means of gaining strategic advantages over rivals (Choucri and Clark 2018, 364). In what forms is cyberpower projected and accumulated? The answer rests with the concept of *cyberconflict*.

The Rise of Cyberconflict and Cyberwar

The concepts of cyberconflict and cyberwar began their rise to prominence with John Arquilla and David Ronfeldt's 1993 article "Cyberwar is Coming," which was written within the strategic context of the mid-1990s and heralded a new era in strategic thinking—a revolution in military affairs (Arquilla and Ronfeldt 1997, 27–31). Since then, discourse about cyberwar has gradually shifted from its disruptive effects on information and communication technologies (ICTs) to its potential to cause the physical destruction of critical infrastructure, especially after the Stuxnet incident in 2010 (Harknett and Smeets 2022, 536–37). Jason Healey (2013, 17–20) dubs this new phase the "militarization" period of cyberwarfare; its emergence represents a paradigm shift from the information warfare of the 1990s to cyberwar, and marks the growing strategic saliency and destructiveness of cyberoperations in the US (Haizler 2017, 32–37).

Existing conceptualizations of cyberconflict exhibit little divergence. For example, Healey (2013, 15) defines cyberconflict as "when nations and non-state groups use offensive or defensive cyber capabilities to attack, defend, and spy on each other, typically for political and other national security purposes." Others conceptualize it as

"the use of computational technologies for malevolent and destructive purposes to impact, change, or modify diplomatic or military interactions" (Valeriano and Meness 2015, 21). Although Healey's definition places greater emphasis on the defensive aspects of cyberconflict, the fundamental distinction between these definitions lies in the actors involved. The latter implies that cyberconflict is contested by states, as "diplomatic or military interactions" are the province of states, and nonstate actors have a limited capability to exert a meaningful effect on these interactions—a definition consistent with Valeriano and Meness's state-centric approach (Valeriano, Jensen, and Maness 2018, 2–17).⁴

In cybersecurity scholarship, cyberconflict serves as an umbrella term for "cyberwar," which is misused as a broader concept due to the disproportionate attention that policy and academic circles give to destructive cyberoperations (Harknett and Smeets 2022, 534; Healey 2013, 14). More inclusive in scope, cyberconflict encompasses almost all cyberstrategies or politically motivated cyberactivities affecting national security (Craig and Valeriano 2018, 87; Valeriano and Maness 2017, 262).⁵

Scholars theorize three generic cyberstrategies: disruption, espionage, and degradation. States employ these for various purposes, such as shaping the behavior of other actors through coercion and improving their relative power. Disruption tends to be unsophisticated and aims to influence the decision making of a target through harassment (e.g., the defacement of the Georgian government's websites during the 2008 Russia–Georgia conflict). Cyberespionage, however, is stealthier and more sophisticated. It aims to achieve strategic advantages over adversaries and shift the interstate balance of information by infiltrating their computerized systems to gather intelligence (e.g., China's attempts to steal the F-35 design plan). Unlike cyberespionage, cyberdegradation aims to mold the payoff structure of opponents by destroying their essential capabilities. Degradation is more advanced, resource intensive, damaging, and coercive in nature. Cyberwar falls into this category and may cross the threshold for "armed conflict," potentially influencing interstate power balances (Harknett and Smeets 2022, 534; Valeriano, Jensen, and Maness 2018, 36–41).

Using Stuxnet as a case, I define cyberwar as destructive cyberoperations conducted by a nation "against its adversary nation's critical military or civilian cyber networks and systems with an aim of coercing adversaries and extracting political concessions by inflicting physical damage on these computers, computer systems, and networks," with such damage possibly, but not necessarily, including injury and death, or total destruction (Akdağ 2019, 228–29). Cyberwar is exclusively a type of state-to-state cyberconflict because only states possess the capabilities to conduct such operations. It is nonkinetic, but can cause physical destruction to yield concessions from the enemy or to

“assert status in international relationships and to teach lessons to other countries” via coercion (Libicki 2009, 121; see also Liff 2012, 404–8). Therefore, cyberwar is politically motivated cyberbellicosity, as exemplified by Stuxnet, which may have been employed to maintain the balance of power in the Middle East by disrupting the Iranian nuclear program (Akdağ 2017, 114–15).

However, conceptualizing cyberwar has prompted great debates among scholars, particularly over whether the incentives for cyberoffensive strategies outweigh those for defensive ones (Gartzke and Lindsay 2015; Saltzman 2013; Slayton 2017).⁶ The discussion about the offense-defense balance in cyberspace is intellectually rooted in DR’s offense-defense theory, which explains why pro-status quo states engage in war. The theory postulates that military technology geared toward offensive action makes it easier to attack than defend, increasing the odds of war. Structural modifiers (e.g., the mobility of military technology and proximity of targets) can affect the offense-defense balance. The closer the enemy is and the more mobile the offensive technology, the more incentives there are to attack (Jervis 1978; Van Evera 1998).

Some scholars who have applied offense-defense theory to cyberspace argue that cyberconflict offers more incentives for offense than for defense (Gartzke and Lindsay 2015, 316). They do so for four reasons. First, acquiring and employing offensive cybercapabilities is easy and cost effective compared to conventional weapons. Second, cyberspace provides a target-rich environment where everything online is vulnerable to attack. Third, conventional aggression mitigators (e.g., territorial distance) are absent in cyberspace. In this sphere, offensive actions have an instantaneous impact, which grants the first mover strategic advantage (Slayton 2017, 77–81; Wilner 2020, 254). Lastly, cyberspace offers anonymity to aggressors, further incentivizing attack over defense.

Other scholars contest this view. They maintain that offensive cyberoperations are neither cheap nor easy to deploy. Stuxnet, for example, took several years to develop and execute due to its complexity, and cost hundreds of millions of dollars (Valeriano and Maness 2017, 266). Erik Gartzke and Jon Lindsay (2015) argue that deception strategies (e.g., honeypots) are more advantageous than offensive strategies in cyberspace. Critics challenge the effectiveness of cyberweapons, as they are not capable of disarming an adversary, negating the so-called first-mover advantage of cyberoffense (Slayton 2017, 78–80). While analyzing the offense-defense balance in cyberspace remains an empirical challenge, the perceived dominance of offense appears to be commonplace in great power cybersecurity relations, as substantiated in the 2018 US National Cyber Strategy (Gartzke and Lindsay 2015, 338–340; The White House 2018).

Although cyberconflict seems to favor offensive strategies, it does not fully correspond to OR’s assumptions. For

example, the nonterritoriality of cyberspace brings actors into continuous contact with one another, which complicates the geopolitical calculations that states make. Therefore, I assess the empirical relevance of OR by testing if its assumption about hegemonic expansion applies to cyberspace, and offer conceptual amendments that adapt OR to the realities of this sphere. I begin by comparing OR with DR, clarifying the distinctions in their understandings of the conditions for conflict and peace in the international cybersystem.

Offensive and Defensive Realism

Offensive realism and defensive realism are different branches of structural realism, but they share core assumptions about the ontology of international politics. Both explain systemic outcomes (e.g., war) and state behaviors (e.g., American grand strategy), describe the political structure of international system as anarchic, and consider this anarchy to be the main driver of international conflict (Taliaferro 2001, 132–40; Waltz 1979). This anarchical structure is infused with uncertainty because states, as primary and rational actors, distrust the intentions of other states and fear their offensive capabilities. Consequently, states are incentivized by the structure to take self-help measures to increase their relative power and security for survival (Mearsheimer 2001a, 30–32).

Notwithstanding their ontological overlap, OR and DR differ in their understandings of how anarchy influences state behavior, leading to distinct conclusions and policy prescriptions. Kenneth Waltz’s (1979, 126) DR attributes international conflict to unrelenting competition between states, which seek security but misinterpret the same security-seeking behavior by peers as threatening, resulting in an unresolved paradox of interstate relations: the security dilemma (Jervis 1978). DR defines states as security seekers concerned with maintaining the status quo via balancing, a default security strategy to deter and fight belligerent states. DR’s bias toward the status quo stems from its presumption that aggressive attempts to accumulate power are self-defeating, since they will provoke countervailing attempts by other status quo seekers (Mearsheimer 2001a, 209–11; Snyder 2002, 151–52; Waltz 1979, 126). Thus, Waltz deems a balancing countermove to be an effective deterrent mechanism against aggression (Ripsman, Taliaferro, and Lobell 2016, 38; Toft 2005, 385; Walt 1985, 13–14).

In contrast, John Mearsheimer’s OR explains interstate conflict as a phenomenon driven by fierce competition between power-maximizing expansionist states. Mearsheimer (2001a, 21–36) believes that anarchy causes great powers to be aggressive, revisionist, or expansionist, because it gives them incentives to increase their security by accumulating power, using offensive strategies whenever possible. Importantly, Mearsheimer disputes that balancing is an effective conflict prevention mechanism

Table 1
Offensive Realism's View of Hegemons and Hegemony

Characteristics of Mearsheimer's hegemon	<i>Regional</i> : concentrating power and resources only within its own region <i>Secured</i> : protected by unrivaled material power capabilities and the ability to project them, and/or by defensive topographical barriers <i>Reluctant/status quo seeker</i> : no further expansion into or direct intervention in remote regions
--	--

because states cannot be certain about the right amount of power needed to preserve the existing balance of power, and because balancing is undermined by collective-action pathologies (e.g., free riding) (34–35; Brooks and Wohlforth 2008, 35–36). Consequently, he contends that major states seek to balance only in rare circumstances. The case in point is Mearsheimer's "poster child America" (Layne 2002, 120), which joined World War II only after the Pearl Harbor raid, when the threat posed by Japan proved to be existential (Mearsheimer 2001a, 181).

Given the challenges to the strategy of balancing, Mearsheimer proposes "regional hegemony" for great powers to effectively prevent and deter aggression and ensure security and survival (Mearsheimer 2001a, 140–44). He conceptualizes a hegemon as the most powerful nation in a region, with a capacity to exert control or influence over the actions of others. The source of hegemonic power is mainly unrivaled military, economic, and political capabilities, or a combination thereof. Accordingly, a state becomes a hegemon when it is "the only great power in the system," enabling it to dominate that system. Mearsheimer's understanding of *hegemony* is then equated with overwhelming material capabilities and their use for coercive purposes (40–41).

Crucially, Mearsheimer (2001a, 40–42) opposes global hegemony because natural constraints like oceans prevent extraregional power projection. Japan in East Asia and the US in North America exemplify regional hegemons that ensure security in their hinterlands by concentrating power locally, instead of making expensive extraregional commitments (Kirshner 2012, 60–61).⁷ OR's thesis about regional hegemony informs its vision for great powers: the aim of power-seeking states is ultimately to achieve regional hegemony using offensive strategies under appropriate strategic circumstances. Only after achieving hegemony can major powers guarantee their survival and transform from power maximizers into status quo seekers or *reluctant* hegemons. In doing so they deter aggression, because rational states avoid conflict with stronger rivals due to the greater chance of defeat (Layne 2006, 17–26; Mearsheimer 2001a, 37–43, 169–219; 2001b, 46).

Table 1 outlines the defining features of Mearsheimer's theory of hegemony and his controversial prediction for the US. His theory predicts that the US would be a *reluctant* hegemon once it has secured a preponderance of regional power, after which it would stop expanding and

become a status quo power, seeking to prevent and deter counterhegemonic aspirations outside its hegemonic sphere of influence by adopting buck-passing or offshore-balancing strategies (Layne 2006, 17–26).

However, I argue that the same balance-of-power mechanism may not apply to state-to-state cybersecurity strategies. Thus, prior to testing OR's assumption, its view of "hegemony" needs conceptual refinement because cyberspace is incompatible with our traditional understanding of concepts such as war (Rid 2012).

Reconceptualizing Hegemony

As discussed above, OR associates hegemony with overwhelming material capabilities and the ability and desire to project them. Because the US exhibits these features in the kinetic world, it qualifies as a hegemon in this sphere. Such a power-centric premise applies to cyberspace too, as cyberhegemons can be characterized by their unrivaled cyberwarfare capabilities and their use of these capabilities for coercive purposes. To accommodate the intricacies of cyberspace, however, it is necessary to modify OR's framework regarding hegemonic expansion and the level of security OR assumes a hegemon enjoys.

The first such modification concerns OR's preference for regional rather than global hegemony. For Mearsheimer (2001a, 32–42), interstate competition causes actors to aggressively pursue regional hegemony to secure their own survival. Regional hegemony is more attainable, as it entails controlling a specific region via superior power, fulfilling the imperatives of a self-help system that stresses security and sovereignty over cooperation. Conversely, Mearsheimer considers the pursuit of global hegemony to be self-defeating because it risks overstressing resources and making costly commitments that no state can afford. This is particularly due to natural barriers that render extraregional power projection unfeasible, and which have caused the demise of great powers that have overlooked this fact (e.g., Napoleonic France).

However, Mearsheimer's preference for regional hegemony is based on premises that do not apply to cyberspace, a domain whose unbounded, decentralized, and interconnected characteristics remove geographical barriers and create continuous contact among actors. This minimizes the constraining effects of geopolitics on expansionist states, making global power projection practical, cost effective, and often instantaneous (Healey 2019, 1; Rid

2012, 8). In cyberspace, great powers do not have to make expensive commitments, mobilize extensive resources such as tanks and soldiers, or cross vast oceans or harsh topographies to engage in conflict; global interconnectivity ensures that the enemy is just one click away, eliminating the risk of self-depletion. Consequently, major states are structurally incentivized to pursue global, not regional, cyberhegemony via offensive, expansionist cyberstrategies. Given the relative feasibility of cyberpower projection, a cyber version of OR suggests that big powers would be better off seeking global cyberhegemony to achieve deterrence and security in cyberspace. This adjustment to the concept of hegemonic expansion in cyberspace will be tested using the US as a case study.

The second modification addresses the degree of security that OR assumes regional hegemons enjoy. Mearsheimer (2001a, 34–42) expects the US, as a regional hegemon, to transform from a power-seeking, expansionist state into a *reluctant* hegemon that seeks to preserve the status quo, secured by its formidable material capabilities and by natural barriers that isolate it from major competitors. To maintain this power position, OR predicts that the US will deter bids in distant regions to counter its hegemony via buck-passing or offshore-balancing strategies (Layne 2006, 17–26). However, cyberconflict challenges OR’s notion of a *secure* and *reluctant* regional hegemon for two interconnected reasons.

First, the US is less secure in cyberspace, as the non-territoriality of cyberspace invalidates the defensive advantages its geographical location provides. Second, while internet connectivity augments American hegemonic power, it also leaves the US more susceptible to cyberthreats than less-wired states (Kesan and Hayes 2012, 443). Former president Barack Obama (2009) underlined this paradoxical situation: “It’s the great irony of our Information Age—the very technologies that empower us to create and to build also empower those who would

disrupt and destroy. And this paradox—seen and unseen—is something that we experience every day.” Obama’s last sentence also reflects the clandestine nature of cyberthreats, as system and network intrusions may go undetected. For example, US House representative Michael McCaul suspected China of deploying logic bombs—malicious code that lies dormant until needed—in American infrastructure to use in times of conflict. This insecurity underlies the Assumed Breach paradigm governing cybersecurity discourse (Lindsay 2015, 7).

The White House’s 2018 National Cyber Strategy also recognizes the vulnerability of critical US infrastructure to cyberattacks (The White House 2018, 2–3). This uncertainty, coupled with its high degree of internet connectivity, makes the US a relatively *insecure* and more *vulnerable* hegemon in cyberspace. To deter cyberthreats and achieve cybersecurity, then, Washington can be expected to pursue global cyberhegemony through constant expansion and cyberpower maximization, and not seek to preserve the status quo as a reluctant regional hegemon.

Table 2 demonstrates how the modified version of OR conforms to the realities of cyberspace. Based on table 2, I define global cyberhegemony as a power position in which a state is perceived to possess overwhelming offensive and defensive cybercapabilities, and seeks to project its cyberpower globally to achieve security and deterrence in cyberspace. Can the US dominate cyberspace via cyberhegemony? Cyberdominance means that a state has the ability to achieve and maintain a superior position from which it can effectively disrupt, destroy, control, and influence others’ cyberactions. Empirical data suggest that the US’s cybersecurity paradigm is relatively effective, as Washington has achieved escalation dominance by extracting the most concessions from its cybercompetitors, including China, using offensive cyberstrategies (Valeriano, Jensen, and Maness 2018, 82).⁸ To achieve and maintain global cyberhegemony, the US can concentrate on upgrading its digital

Table 2
Comparative Analysis of Offensive Realism’s Views on Hegemony

	Hegemony in the kinetic world	Hegemony in cyberspace
Scope of hegemony	<i>Regional</i> : power and resources concentrated only within the hegemon’s own region due to the high cost and impracticality of global power projection	<i>Global</i> : extraterritorial projection of cyberpower via offensive strategies due to the relative feasibility and low cost of extraregional cyberpower projection
Level of security	<i>Secured</i> : protected by unrivaled material power capabilities and the ability to project them, and/or by defensive topographical barriers	<i>Insecure/vulnerable</i> : threatened by the boundless and interconnected features of cyberspace and the opaque nature of cyberthreat
Intention	<i>Reluctant/status quo seeker</i> : no further expansion into or direct intervention in remote regions	<i>Ambitious/expansionist</i> : constant expansion, intervention, and cyberpower seeking on a global scale

infrastructure via research and development, artificial intelligence, and quantum computing. Although technological leadership could theoretically secure cyberdominance for Washington, it remains to be seen whether the US can achieve such dominance given the fluidity of cybertechnology.

However, not all states can afford to pursue global cyberhegemony. Cyberspace offers easy access to the playing field, but cyberpower is not cheap to acquire. There may be significant temporal, organizational, and resource constraints to pursuing a preponderance of cyberpower. For instance, Stuxnet took years to develop, cost over \$300 million, and required the cooperation of two countries. Therefore, while producing cyberpower is cost effective relative to conventional and nuclear power, it still carries considerable costs that not all cyberactors can afford (Slayton 2017, 84–90; Valeriano, Jensen, and Maness 2018, 36–41).

Defensive Realism as an Alternative Explanation

As previously noted, Waltz's DR treats expansionism and aggression in world politics as counterproductive due to the prospect of balancing countermoves against potential hegemonies (e.g., the alliances against Germany in World War I and World War II) (Rendall 2006, 523–24). For DR, therefore, stability rests on an interstate power equilibrium. Based on this balance-of-power perspective, DR argues that the US will avoid pursuing global cyberhegemony even in the absence of strategic restraints on the expansion of its cyberpower, as Washington would likely encounter an antihegemonic cyberalliance that would defeat its security-seeking purpose. This situates DR as an alternative framework to OR in explaining how states seek security and power in cyberspace—whether via expansion or via the balance of power.

However, I argue that DR's framework has poor explanatory power in cyberspace. A counterhegemonic balancing strategy is unlikely to serve as a structural limitation on expansion in cyberspace because the nature of cyberpower and cyberconflict exacerbates the difficulties involved in achieving a balance. These balancing problems—including those unique to cyberspace—pose considerable risks and challenges to states, reducing the likelihood of effective countermoves. I identify four such problems below.

First, the opaque nature of cyberpower may make it harder for states to judge the cybercapabilities of other states, complicating attempts to balance against cyberthreats. Mearsheimer (2001a, 2–21) raises this crucial point when he expresses skepticism about the prospects of forging a successful counterhegemonic coalition—a strategy undermined by the impracticality of assessing whether coalition partners have the right amount of power needed to achieve equilibrium and by other balancing flaws (Sheldon 2011, 100). This uncertainty is even

greater in cyberspace as shifts in the interstate balance of cyberpower can occur faster due to the adaptability and volatility of cybertechnology.

The Belfer Center's National Cyber Power Index (Voo et al. 2020; Voo, Hemani, and Cassidy 2022) underlines the fluidity of interstate cybercapabilities. The index's comparative analysis shows that Russia's cybercapabilities overtook those of the United Kingdom within just two years—a rapid shift compared to conventional power transitions (consider the decades taken by China to catch up with the US economically) (Voo, Hemani, and Cassidy 2022, 10–12). This volatility creates extra uncertainty, increasing cyberthreat perceptions among great powers such that they assume worst-case scenarios. This in turn drives them to maximize their cyberpower via expansionist strategies, and ultimately to seek global cyberhegemony to preserve their cybersecurity and deter potential cyberthreats. Such dynamics undermine cyberstrategies based on the balance of power, which has implications for CPT's core concepts and assumptions, as I will discuss below.

Second, counterhegemonic balancing may fail in cyberspace because cyberalliances risk entangling great powers in the conflicts of other states. Small states may draw larger alliance members into war by provoking major cyberadversaries, just as the conflict between Austria and Serbia in World War I evolved into a war between Austria, Germany, Serbia, and Russia. Hypothetically, a small state conducting punitive cyberstrikes against China could trigger a kinetic retaliation; and if the state were a member of NATO, the organization's Article 5 provisions could draw the US into a major conflict and/or cyberwar with China, undermining collective attempts to balance against common cyberthreats and incentivizing cyberpower maximization and expansion for cybersecurity (Libicki 2019, 10–11). Correspondingly, the cybersecurity of a member of a counterhegemonic cyberalliance is integral to the security of the rest due to the interconnectedness of cybersystems. To illustrate, if the Five Eyes alliance became a cybersecurity coalition, the US could be dragged into a cyberwar with China when an alliance member faced a cyberthreat from Beijing. Neutrality would be unlikely to be an optimal option given the coalition's cybersecurity interdependence, rendering balancing against hegemonic cyberpowers a risky strategy and diminishing the efficiency of Waltz's balance of power.

Finally, the nature of cyberconflict may negate the benefits of coming together for collective defense and deterrence. A negative correlation exists between the size of a cyberalliance and its effectiveness, as adding members amplifies vulnerabilities that can be exploited, deepens the challenges involved in defending the alliance's systems, and potentially decreases the quality of the alliance's cybercapabilities due to differences in training levels. The volatility of cybertechnology (e.g., the loss of a cyberweapon's effectiveness once it is exposed) can also

discourage states from sharing cybercapabilities against a common cyberthreat. Additionally, counterhegemonic cyberbalancing may be undermined by the mistrust that lingers even within cyberalliances, since states spy on each other in cyberspace, as evidenced by the Snowden revelations (DeVore and Lee 2017, 45; Libicki 2019, 3–11).

To recap, counterhegemonic cyberbalancing as a security mechanism is unlikely against expansionist great powers due to the characteristics of cyberpower and to difficulties in achieving a balance. This offers structural incentives for states to maximize their own cyberpower—rather than balance against that of others—as the costs of expansion are not prohibitive in cyberspace. The empirical assessments made in the next section reinforce this conclusion.

Because the dynamics of the balance of power do not operate in cyberspace and counterhegemonic balancing is unlikely, there are no structural barriers preventing major states from seeking global cyberhegemony. As such, the dominant behavior in cyberspace becomes one of expansion and power maximization for cybersecurity given the minimal risks and costs involved. Major states, including the US, risk undermining their cybersecurity if they do not constantly pursue power and advantage as incentivized by the structure of cyberspace. Within the boundless and unsecured domain of cyberspace, opportunities that are not seized are ceded to adversaries, risking national security both within and through cyberspace.⁹

OR's analytical value and its theoretical relevance to cyberspace is not entirely contingent on the modified concept of hegemony outlined above. Mearsheimer's core assumptions remain valid in cyberspace, as secrecy, uncertainty, mistrust, and the perceived advantage of offense dominate cyberengagements (Mearsheimer 2001a, 31–32). Uncertainties about relative cybercapabilities and intentions shape states' policies toward other cyberactors (e.g., strategic cyberdeterrence) (Valeriano, Jensen, and Maness 2018, 41). Scholarship acknowledges the anarchical characteristics of cyberspace, which lacks conflict prevention tools (such as interstate cooperation), well-established cyber-specific laws, and a global system of governance.¹⁰ Consequently, mutual fear and cyberinsecurity guide the actions of states in this sphere, causing cyber arms races and eventually cyberconflict. For example, Craig and Valeriano (2016, 146–51) find that both Iran and the US build cyberarms due to feelings of mutual fear and cyberinsecurity, which have been exacerbated after Stuxnet. While the extent to which cyberspace can be defined as anarchical is disputable, OR appears well equipped to explain how the dynamics of cyberanarchy affect state-to-state cybersecurity interactions.¹¹

Testing Offensive Realism's Assumption of Hegemonic Expansion in Cyberspace

This study aims to examine whether OR's theoretical and conceptual tools offer a plausible and empirically relevant

understanding of interstate security relations in cyberspace. I qualitatively evaluate whether OR's thesis about hegemonic expansion holds in the virtual domain using the US as a case study. Mearsheimer (2001a, 140–46) contends that great powers exercise influence and power only within their region, as doing so across topographical barriers entails costly economic and military commitments that impose strategic restraints on extraregional power projection. Mearsheimer therefore favors regional but not global hegemony to avoid self-depletion, implying that without such barriers, great powers would pursue global hegemony. If he is correct, the US should seek to expand its cyberpower and influence globally due to the absence of these constraints in cyberspace.

To examine whether Washington has been seeking global cyberhegemony, I analyze the US's major declaratory cyberpolicies and cyberstrategies from 2003 to 2023, as well as the Stuxnet and Snowden incidents. This analysis seeks to establish whether the US has intended to expand its cyberpower and influence beyond its hinterland by adopting offensive cyberstrategies. Exercising power and influence in cyberspace can take many forms. Washington's cyberdiplomacy with countries outside its region indicates its commitment to expanding its global reach; the US's attempts to establish international cyber-specific norms and promote American ideological values (e.g., the free flow of information) signifies an interest in shaping the global governance of cyberspace; and the worldwide operations of US-based ICT corporations (e.g., Google) and the cyberinterventions of the US Department of Defense (DoD) across multiple regions reflect the US's ambition to maintain influence, control, and power beyond its back yard.¹²

Examining the Stuxnet and Snowden cases serves two purposes: to underline Washington's offensive cybercapabilities and its intention to shape events and outcomes in the international cyberecosystem, and to demonstrate whether the US's behavior in cyberspace conforms to its cybersecurity doctrines. Before moving on to these cases, I first examine the US's major declaratory cybersecurity policies to establish whether it has clearly articulated hegemonic ambitions in cyberspace.

Analyzing Major US Cybersecurity Policies (2003–23)

The Bush administration's National Strategy to Secure Cyberspace, launched in 2003, represents a significant milestone in the evolution of the US cybersecurity paradigm. Although it has multiple purposes, its primary function is to advise US leaders on how to address global cybersecurity issues via international cooperation: "America must be ready to lead global efforts, working with governments and industry alike, to secure cyberspace that is vital to the operation of the world's economy and markets" (The White House 2003, 49). This signifies

the US's intent to create global cybersecurity standards and expand its influence in cyberspace.

However, despite suggesting greater American hegemonic leadership in cyberspace, the document avoids overtly endorsing aggressive US expansion in this domain at the expense of its rivals. Instead, it highlights defensive and denial measures for safeguarding national cyberinfrastructure, makes vague references to interstate punitive cyberstrategies, and calls for the prosecution only of transnational cybercrimes (The White House 2003, 49–40; Wilner 2020, 257). Anticipating potential blowbacks against innocent parties made vulnerable by global interconnectivity, the Bush administration deemphasized aggressive cyberstrategies (Wilson 2004, 10). Thus, the US's cybersecurity paradigm favored defense over offense during the 1990s and early 2000s.

However, offensive cyberstrategies in the US's cybersecurity thinking began to rise to prominence during the Obama administration. A key indicator of this was the creation of US Cyber Command (USCYBERCOM) in 2010. Initially commissioned with protecting US government's cybersystems and cybernetworks, USCYBERCOM would later expand to develop offensive cybercapabilities and conduct offensive cyberoperations (US Department of Defense 2018; Wilner 2020, 259–61).

In 2011, the White House and DoD broadened the country's cybersecurity doctrine with the "Strategy for Operating in Cyberspace." It identifies five strategic initiatives, including treating cyberspace "as an operational domain" and working with allies to reinforce "collective cybersecurity" via cyberdeterrence (US Department of Defense 2011, 1–9). While USCYBERCOM constituted the DoD's main conduit for offensive cyberstrategies, the 2011 document did not clearly link the US's cyberdeterrence posture to aggressive cyberstrategies but rather prioritized defense and denial measures and related lexicon (e.g., restrain and resilience).

Correspondingly, the DoD's 2011 doctrine did not embrace ambitious, aggressive cyberstrategies to expand American influence abroad, but rather highlighted cyber-norms, collective self-defense with allies (e.g., enhancing "warning capabilities"), and the security of cyberspace: "DoD will assist US efforts to advance the development and promotion of international cyberspace norms and principles that promote openness, interoperability, security, and reliability" (US Department of Defense 2011, 9–10). Yet in the 2013 Task Force Report, the DoD suggested a gradual strategic shift from defense to offensive cybercapabilities and nuclear deterrence to protect vital interests and deter bellicose cyberactors via punishment (Wilner 2020, 261–62).

In the 2015 DoD Cyber Strategy, the strategic language still favored a "doctrine of restraint" but signaled a shift toward offensive cyberoperations, including retaliatory strikes against adversaries. In previous documents, the

DoD had underlined defensive (e.g., firewall) and denial (e.g., resilience) cybercapabilities to counter cyberthreats, but the 2015 strategy indicated Washington's intent to confront cyberattacks against American interests "at a time, in a manner, and in a place of our choosing, using appropriate instruments of US power" (US Department of Defense 2015, 11). It outlined offensive tasks for USCYBERCOM as well as DoD plans to incorporate offensive cybercapabilities into military operations. The document highlighted the strategic significance of the Cyber Mission Force, which was created between 2012 and 2013 to counter cyberthreats and defend American interests in cyberspace. The 2015 strategy stated that the Cyber Mission Force would have a personnel of over six thousand once fully operational, aligning with its goal of building and maintaining US mission capabilities in cyberspace (US Department of Defense 2015, 6–11; Wilner 2020, 262–65).

The DoD's shift toward developing more offensive capabilities was driven by the strategic context of the time. The 2015 document identified Russia and China as dangerous competitors developing sophisticated cybercapabilities to undermine US interests (US Department of Defense 2015, 6–11). To address this, the 2015 strategy reiterated the need for US leaders to build cybercapacity with allies and secure critical infrastructure, including military and government networks. But it limited the US's global involvement in collective cyberdefense and cyberoffense operations to "priority regions" (e.g., Asia-Pacific) that have historically been pivotal to American grand strategy (US Department of Defense 2015, 26–28).

The rise of offense-leaning concepts in US cyberpolicies since the Obama administration has been accompanied by empirical precedents. The discovery of Stuxnet in 2010, Edward Snowden's revelations in 2013 about the aggressive use of National Security Agency (NSA) cybercapabilities, and American cyber-retaliation against North Korea for its cyberattacks against Sony Pictures in 2014 are prominent cases (Mazzetti and Schmidt 2013; Wilner 2020, 263–64).

These examples demonstrate a mismatch between the US's declared policy of operational "restraint" and its cyberpractices between 2010 and 2014. During these years, USCYBERCOM aggressively used its capabilities to disrupt and destroy the cybersystems of both adversaries and allies, as the Snowden revelations and Stuxnet made clear. These practices indicate that the US did not in fact adhere to the "doctrine of restraint" or largely allow adversaries' cyberbellicosity to go unpunished in the 2010–14 period, contrary to the findings of CPT analysis of US cyberpolicy during the same years (Fischerkeller, Goldman, and Harknett 2022, 131–32).

Yet the US's 2018 cyberpolicies conspicuously prioritized offensive cyberstrategies, such as preemptive cyberattacks, to slow the rise of challengers and expand

American influence globally. Such a dramatic shift reflected a recognition that the traditional deterrence paradigm (and its doctrine of restraint) in American strategic cyberthinking was limiting the US's ability to further its national interests in cyberspace. This view was reinforced by the DoD's anticipation of prolonged strategic cybercompetition with China and Russia, two adversaries that have persistently sought to undermine the power of the US and its allies. To maintain the US's military overmatch and safeguard American interests, the DoD adopted two strategies combining offense and defense: "persistent engagement" and "defend forward." These strategies aimed to proactively engage with and disrupt malicious cyberactivities at their source, persistently counter cyberthreats, and degrade adversaries' capabilities and networks (Fischerkeller, Goldman, and Harknett 2022, 128–40; US Cyber Command 2022; US Department of Defense 2018, 2–4).

Within the "persistent engagement" framework, USCYBERCOM leads efforts to execute cybermissions and achieve and maintain American superiority in cyberspace. At the Department of Homeland Security's 2018 Cybersecurity Summit, Vice President Mike Pence (2018) confirmed that the US's intention was to achieve cyberhegemony: "Our goal remains: American security will be as dominant in the digital world as we are in the physical world."

As the first fully articulated national cyberpolicy, the Trump administration's US National Cyber Strategy, launched in 2018, complements USCYBERCOM's vision. It tasks cyberwarriors with maintaining peace and cybersecurity via "strength," cyberpower preponderance, and cooperation with US allies. The policy stresses Washington's primary goal: to "[i]dentify, counter, disrupt, degrade, and deter" cyberactivities that jeopardize US national interests while maintaining cyberdominance (The White House 2018, 20–26). Consistent with this hawkish posture, it threatens to impose "swift and transparent consequences" on those who challenge American interests in cyberspace (The White House 2018, 21).

Furthermore, the document champions the expansion of US global influence and encourages the country to "launch an international Cyber Deterrence Initiative" with allies to punish cyberbellicosity and deliver a deterrent message to adversaries. It also seeks to uphold the US-held values of "an open, interoperable, reliable, and secure Internet" as well as the multistakeholder model in cyberspace, reaffirming the country's commitment to expanding its extraregional influence (The White House 2018, 20–24).

The Biden administration's National Cybersecurity Strategy, launched in 2023, largely represented continuity with the ambitious and aggressive posture of 2018 that embraced global US cyberhegemony. The document advocates maintaining US superiority in cybertechnology and innovation. It reaffirms the US's commitment to

working with allies to build collective cybersecurity, establish cybernorms, punish violations, and protect US-held values (e.g., individual liberty) against "the dark vision for the future of the Internet" advocated by autocratic regimes such as China (The White House 2023, 29). The strategy addresses steps to expand the US's influence and leadership, such as the 2022 Declaration for the Future of the Internet (US Department of State 2022), to maintain and reinforce the US-sponsored internet governance regime.

However, the Biden administration changed the nature of American assistance to countries under cyberattack, such as Ukraine (The White House 2023, 2–7). The US extended its help beyond defensive efforts to include offensive measures against cyberaggressors, clearly demonstrating its interest in acting as a global cybersecurity provider through an offense-based strategy (The White House 2023, 28–31). In parallel, the Biden administration demanded an updated "defend forward" approach. Consequently, the DoD published a two-page summary of its 2023 cyberstrategy and pledged to "maximize its cyber capabilities" for "integrated deterrence." It reaffirmed "hunt forward" cybermissions "to disrupt and degrade" adversaries' capabilities and reiterated a desire to collaborate with allies to increase cybercapacity and safeguard cyberspace, signaling the US's intention to dominate interstate cybersecurity competition via offensive strategies (US Department of Defense 2023).

The US's major cyberpolicies from 2003 to 2023 demonstrate that Washington has been seeking extraterritorial expansion of its cyberpower and influence. It aims to achieve global cyberhegemony primarily by exercising offensive cybercapabilities to maximize its cyberpower, deter cyberadversaries, and ensure its cybersecurity. Especially since the Obama administration, Washington has grown more ambitious, expansionist, and hawkish in its external cyber-relations. It has done so in three ways. First, the US has sought to expand its global reach and hegemonic leadership in cyberspace, primarily through a preponderance of cyberpower and secondarily through internet governance, collective cybersecurity, and technological supremacy. Second, US cyberpolicies emphasize the US's determination to undermine revisionist states (e.g., China) via offensive cyberstrategies (e.g., preemptive strikes). Third, and relatedly, Washington has espoused increasingly ambitious, expansionist, and aggressive cyberstrategies (e.g., "defend forward") that seek to exploit adversaries' cybervulnerabilities to alter or maintain the balance of cyberpower in its favor. In the following sections, I examine Stuxnet and the Snowden revelations to showcase the power and global extent of the US's cybercapabilities.

Stuxnet

The case of Stuxnet is important for several reasons. First, it exemplifies Washington's interest in extraregional

cyberpower projection and its bid for global cyberhegemony using offensive cyberstrategies. Second, Stuxnet shows that the US's cyberbehaviors are consistent with its hawkish cybersecurity policies. Third, Stuxnet demonstrates the superiority of the US's cyberwarfare capabilities over those of other countries, a sign of hegemonic power. Fourth, it details the nature of hegemonic cyberconflict.

Stuxnet epitomizes Washington's willingness to exercise cyberpower to achieve global outcomes. Uncovered in 2010, Stuxnet was developed under the Bush administration in 2006 as a part of Operation Olympic Games, a program to target the Iranian nuclear facility at Natanz without a kinetic attack. Initially, the NSA and the Central Intelligence Agency (CIA) collected intelligence on the facility's systems to identify vulnerabilities. American agencies then collaborated with their Israeli counterparts to create a sophisticated and malicious code that exploited these vulnerabilities, which would later come to be known as Stuxnet. Stuxnet's deployment was authorized by the Bush administration in 2008, but the Obama administration intensified efforts to ensure Stuxnet's success, demonstrating the US's long-term strategic shift toward offensive cyberstrategies and extraregional cyberpower projection (Jenkinson 2021, 19–24; Sanger 2012, 110–29).

Stuxnet has distinctive characteristics that illustrate Washington's cyberwarfare capabilities and technological prowess. The first concerns its level of sophistication. Cybersecurity expert Robert McMillan called Stuxnet one of "the most sophisticated and unusual pieces of software ever created" (quoted in Farewell and Rohozinski 2011, 23). Stuxnet exploited four "zero-day vulnerabilities" (undiscovered loopholes in software) to degrade its target, an accomplishment requiring substantial resources, expertise, and extensive intelligence gathering (Farewell and Rohozinski 2011, 23–25; Lindsay 2013, 365–66). Stuxnet gradually changed the rotation velocity of uranium enrichment centrifuges, eventually causing their physical destruction. Its ingenuity also lay in its stealth, as Iranian cyberoperators remained oblivious until it was too late. Moreover, Stuxnet was programmed to self-destruct once it had completed its mission (Singer 2015, 80–83). Hence, Stuxnet's sophistication and rigorous deployment process demonstrated the US's ability and desire to project its cyberpower globally (Jenkinson 2021, 19–24; Valeriano, Jensen, and Maness 2018, 40).

Stuxnet also offers significant insights into the nature of hegemonic cyberconflict. First, it confirmed that such conflict can have tangible effects outside cyberspace. German security consultant Ralph Langner dubbed Stuxnet a "military-grade cyber missile" targeting Iran's nuclear program (quoted in Farwell and Rohozinski 2011, 23; Lindsay 2013, 366). Second, Stuxnet emphasized the strategic, political, and coercive nature of cyberconflict: it aimed to prevent Iran from obtaining nuclear weapons,

keep the Middle East's balance of power weighed in Israel's favor, and gain political and military advantages over Iran. Third, Stuxnet reflected the coercive aspect of cyberconflict in extracting political concessions. The delay to Iran's nuclear program caused by Stuxnet and the fear of another crippling cyberattack by the US and Israel might have convinced Tehran to sign the 2015 nuclear deal (Akdağ 2017, 121–22).¹³

Stuxnet has not played a central role in advancing US cyberhegemony, but it does illustrate that the US has the superior cybercapabilities characteristic of a hegemonic power. The fact that no cyberoperations like Stuxnet have come to the public's attention since 2010 does not necessarily suggest that the US's cybersecurity paradigm has evolved from coercion to exploitation, as CPT argues (Fischerkeller, Goldman, and Harknett 2022; Mearsheimer 2001a, 40–44). First, cyberoperations are naturally clandestine; they often remain unexposed for years. Stuxnet was discovered years after it had first been deployed. Thus, it is possible that great powers, including the US, may have conducted numerous destructive cyberoperations that have remained unpublicized or undiscovered (Akdağ 2023, 18).

Second, while destructive and coercive cyberoperations dramatically risk escalation, the US appears to have managed escalatory cyberdynamics effectively. As cited above, empirical data indicate that when the US has escalated cyberquarrels, its opponents, including China, have chosen to deescalate, and that the US has acquired more concessions from adversaries by using offensive capabilities (Valeriano, Jensen, and Maness 2018, 82). Therefore it may be erroneous to ascribe the rarity of destructive US cyberoperations merely to a strategic shift toward exploitation. Indeed, CPT theorists admit that their case analysis of the US's cyberstrategy until 2022 indicates that US behaviors do not entirely align with CPT's logic of exploitation and initiative persistence: "Although White House and congressional actions tacitly supported an acceptance of this new paradigm, its core strategic principle has not yet been deliberately and evenly adopted across the whole of government" (Fischerkeller, Goldman, and Harknett 2022, 156). Hence it remains to be seen whether constant expansion or initiative persistence dominates cyberspace, as empirical data emerge over time.

Stuxnet highlights Washington's use of cyberpower to intervene in the affairs of other countries beyond its own region. This extraregional engagement reflects the US's bid for global cyberhegemony using offensive cybercapabilities, an interpretation reinforced by the Snowden revelations.

Snowden Revelations

The Snowden revelations capture the extent of US hegemonic ambitions in cyberspace, detailing covert, offensive US cyberoperations that aimed to expand the US sphere of

influence by projecting US cyberpower across the world. They offer further indications that Washington seeks global cyberhegemony.

In June 2013, Edward Snowden, a former CIA systems analyst and NSA contractor, revealed classified data on global US surveillance operations to journalists Glenn Greenwald, Ewen MacAskill, Barton Gellman, and Laura Poitras, who subsequently reported on the data in the *Guardian*, *Washington Post*, and other publications. The reports indicated that since 2007, the NSA had systematically conducted covert surveillance activities to gather national and international digital data such as phone records (Inkster 2014, 51–54; Landau 2013, 54–58; Wahl-Jorgensen, Bennett, and Taylor 2017, 1–4).

The NSA's surveillance was global in scope, targeting countries across Asia, Europe, Latin America, and Africa. The NSA reportedly infiltrated Chinese public and private networks, including those of the government and businesses, to collect intelligence and identify attack vectors. Even the US's allies and partners were not spared from the NSA's pervasive spying activities. The agency's intrusive cyberoperations included eavesdropping on the computerized networks and communications of foreign embassies and members of the European Union (EU), as well as intercepting the phone calls of the EU's political leaders, including German chancellor Angela Merkel. Reports suggested that the NSA tapped into millions of phone calls in Spain and France and monitored formal and informal communications in friendly Latin American countries such as Chile and Brazil. Turkey, South Africa, Japan, South Korea, and India were also targeted by the NSA's intrusive and offense-orientated cyberactivities, which included cyberdegradation, cyberespionage, and surveillance (Borger 2013; Wahl-Jorgensen, Bennett, and Taylor 2017, 5–6).

Snowden's leaks undoubtedly reveal the US's ambitions to achieve global cyberhegemony via extraregional cyberpower projection to shape international outputs. The revelations disclosed programs to map the global cyberecosystem for real-time intelligence gathering, such as "Treasure Map;" conduct cyberespionage and intrusive surveillance on Americans, allies, and adversaries; and implant malicious code into the networks of adversaries to execute precision cyberattacks on their command-and-control systems. Additionally, they indicate a conformity between Washington's behavior in cyberspace and American cybersecurity doctrines that have increasingly favored ambitious, expansionist, and aggressive interstate engagements. Extraregional US cyberinterventions like those revealed by Snowden reflect Washington's acceptance that it is in strategic competition with adversaries such as China and Russia, and are evidence of its desire to achieve global cyberhegemony through offensive cyberstrategies or hegemonic cyberconflict (Valeriano, Jensen, and Maness 2018, 171–72).

The US has a rich history of offensive cyberoperations (as illustrated by the Snowden revelations), which demonstrates its willingness to leverage its cybercapabilities for strategic ends. The expansion of USCYBERCOM underscores Washington's focus on enhancing its offensive and defensive cybercapabilities and on projecting its power through cyberspace. The US works with international partners and helps to build cybercapacity in allied countries for collective cyberdefense and cyberoffense. Such collaboration serves as a means by which the US can expand its global influence in cyberspace. Strategies such as "defend forward" demonstrate the US's willingness to engage in preemptive actions that neutralize cyberthreats in advance and to operate within adversary networks—offensive postures orientated toward maintaining cyberdominance and preemptively disrupting adversaries. Following a Hobbesian logic, it would be naïve to assume that states would exploit vulnerabilities to seize initiative persistence but not to prepare future attack vectors in case they are needed (Whyte 2018, 529–30). While the 2023 National Cybersecurity Strategy underscored the importance of resilience and defense, it also emphasized the need for offensive measures and for research and development to counter adversaries. The Biden administration's strategy might frame cyberactions as defensive, but it is inherently expansionist in nature. The strategy extends the US's cyberoperations across regions, aligning with its goal of pursuing cyberpower and global cyberdominance (The White House 2023).

The case analysis here concludes that great powers seek cyberpower maximization and expansion rather than initiative persistence to enhance their cybersecurity. Although this analysis and CPT cover US cyberstrategy and policy in the same period, the conclusion I reach here contrasts with that made by CPT scholars (Fischerkeller, Goldman, and Harknett 2022). The distinction arises from how one conceptualizes offensive and defensive actions in cyberspace. A definition of what counts as offensive or defensive cybermeans remains elusive because their characteristics overlap, a function of the fluid nature of cybertechnology. A code can exploit vulnerabilities for offensive and defensive purposes simultaneously: "Moves that are said to be defensive involve forward maneuver that can seem offensive in nature. Offensive operations set to impose costs on the opposition are often thought to be defensive in nature." For example, "the US rerouting of server traffic for a ransomware group" is both an offensive and a defensive operation (Valeriano 2022, 95). While it is "proactive" and occurs in the target's networks, it is also nonviolent and protective of the US's position in cyberspace.

Indeed, the strategy of persistent engagement is offensive at its core, as it requires aggressive actions such as the preemptive disruption and destruction of the cybersystems of would-be cyberchallengers. Brandon Valeriano's (2022,

94–95) reading of Michael Fischerkeller and Richard Harknett’s CPT signals this dual nature and the offense-dominant aspect of their doctrine: “Fischerkeller and Harknett have advocated for the strategic doctrine of cyber persistence because the enemy is persistent and the only way to counteract an adversary’s offensive cyber actions is to take even earlier offensive action.” However, CPT theorists consider cyberactions that seek initiative persistence for security and strategic gains to be inherently exploitative. CPT’s analysis consequently reaches a different conclusion from that of modified OR (Fischerkeller, Goldman, and Harknett 2022, 52).

Conclusion and Implications

Mearsheimer’s theory of offensive realism argues that regional, rather than global, hegemony best serves the goal of ensuring security for great powers because natural obstacles render global power projection costly and extra-regional hegemonic commitments self-depleting. Mearsheimer implies that without such hurdles, the lower cost of extraregional power projection would prompt great powers to pursue global hegemony. Using the US as a case study, I tested this assumption about hegemonic expansion in cyberspace, as the borderless nature of the domain removes strategic restraints on global expansion. If OR’s prediction is accurate, one would expect the US to pursue global cyberhegemony, using offensive cyberstrategies to deter rival powers and ensure its cybersecurity.

I argued that OR has meaningful inferential and predictive power in cyberspace, and confirmed its empirical relevance and analytical ability to explain interstate cybersecurity engagements, specifically cyberdeterrence interactions in hegemonic cyberconflicts. My empirical assessment of the US’s cyberpolicies between 2003 and 2023, the Stuxnet incident, and the Snowden revelations corroborates OR’s assumption that hegemony will seek to expand their power beyond their own regions in cyberspace. Washington pursues global cyberhegemony with an ambitious, expansionist, and cyberpower-maximizing approach to interstate cyberrelations. It engages in agreed competition that falls short of war, particularly with China, to increase its strategic gains while preventing its adversaries from doing the same, to deter malicious cyberactors, and to ensure its cybersecurity through a preponderance of cyberpower (Fischerkeller and Harknett 2019).

This conclusion has significant theoretical and policy implications. First, OR’s empirical relevance in cyberspace may address skepticism about whether realism is applicable to this domain. Second, the empirical analysis substantiates modified OR’s conceptual framework for hegemony that I proposed in table 2. The US pursues global—not regional—hegemony in cyberspace, as the domain presents new conditions, imperatives, opportunities, constraints, and capabilities that incentivize the pursuit of global dominance and challenge DR’s

counterbalancing thesis (Choucri and Clark 2018, 351). My findings substituted Mearsheimer’s *regional, secured, reluctant, and status quo-seeking* hegemon with a *global, insecure, ambitious, and expansionist* cyberhegemon. Security is scarce for the US in cyberspace because the domain’s boundless characteristics nullify the defensive advantages that the US enjoys in conventional space. The US also faces greater vulnerabilities due to its disproportionately high reliance on the internet relative to less-wired nations like China, rendering it a relatively *insecure* and more *vulnerable* hegemon. To reduce its cyberinsecurity and deter cyberthreats, Washington pursues global cyberhegemony by seeking to maximize the degree and reach of its cyberpower, and by preventing its adversaries from making strategic gains and enhancing their own cybersecurity.

Third, the analysis has policy implications for the DoD’s 2018 and 2023 cyberdoctrines, including “persistent engagement,” “defend forward,” and “agreed competition,” which have provoked debates among scholars and policy makers (Klimburg 2020, 107). Some academics argue that cyberdeterrence lacks credibility as a conflict prevention mechanism, and instead propose that the US would be better able to deter cyberadversaries and secure its cybersystems by proactively engaging malicious cyberactors. This proactive engagement requires using cybercapabilities aggressively, such as by neutralizing potential cyberthreats at their origin (“defending forward”). Although it appears escalatory, this strategy could stabilize cyberconflict if actors comply with the norms and rules of agreed competition (Fischerkeller and Harknett 2019). However, other scholars believe the strategy of persistent engagement risks causing a “cybersecurity dilemma” by triggering a cyber arms race, provoking retaliation, or weaponizing information—outcomes that increase cyberinsecurity for both Washington and the international community (Buchanan 2016; Klimburg 2020).

This analysis favors the strategies of “defend forward” and “persistent engagement.” It suggests that the US would be better able to deter adversaries and secure cyberspace if it aggressively used its means to achieve global cyberhegemony. Given the scarcity of security in cyberspace, the US is unlikely to transition from a cyberpower maximizer to a status quo seeker even after achieving global cyberhegemony. Thus, the DoD’s 2018 cyberpolicy positions the US well to meet the particular challenges of cyberspace. Great powers are incentivized by the structure of this domain to pursue cyberhegemony, making interstate cyberrelations competitive and enabling an agreed form of competition that is not bounded by the DR’s balance-of-power DR logic implicit in CPT (Fischerkeller, Goldman, and Harknett 2022, 50). This is where the key distinction lies between modified OR and CPT.

Although both modified OR and CPT are structural theories advocating persistent action in cyberspace, CPT theorists claim that their theory differs from structural IR

theory because states utilize “cyber capabilities for unilateral exploitation, not brute force or coercion” (Fischerkeller, Goldman, and Harknett 2022, 37). Yet the theory’s assumptions and prescriptions implicitly align with DR’s balance-of-power perspective. CPT argues that states seek initiative persistence via exploitative actions—infiltrating into enemy systems through vulnerabilities in these systems—that are calibrated to avoid a kinetic response and aim to achieve favorable cybersecurity conditions through cumulative strategic gains. These gains are contingent upon self-limiting behaviors defining the boundaries of agreed competition, which may be breached by “a relative shift in power between adversaries or a relative decline of a State across the global distribution of power” (Fischerkeller, Goldman, and Harknett 2022, 52). Correspondingly, CPT ties the gaining of power and security to the ability of states to anticipate the relative vulnerability–exploitation balance in cyberspace (24). Here CPT clearly associates the stability of cyberspace or agreed competition with interstate power equilibrium.

CPT’s association of cyberstability with the balance-of-power perspective causes CPT to confront the same problem faced by DR: how can states work out the right amount of power (or strategic gains) needed to maintain the equilibrium?¹⁴ OR argues that this is almost impossible, particularly in cyberspace, where the uncertainty that results from this dilemma is exacerbated by the secrecy of cyberpower and the impact of ever-shifting cybertechnology. Recognizing this, CPT contends that states can only anticipate the balance of initiative. But this would further increase uncertainty, since modified OR asserts that great powers cannot risk their security and survival by engaging in uncertain anticipatory behavior. Indeed, CPT scholars concede that “[t]he substance of cyber agreed competition is currently immature—mutual understandings of acceptable and unacceptable behaviors and of cyber key terrain are maturing slowly and narrowly” (Fischerkeller, Goldman, and Harknett 2022, 50–52). Therefore, they accept that the rules of agreed competition can readily be breached.

Consequently, modified OR argues that states are driven by the structure of cyberspace to assume a worst-case scenario. This assumption is crucial because it explains why states constantly expand their cyberpower and pursue global cyberhegemony for security and strategic gains in cyberspace. Since structural incentives are the same for major states, they tacitly agree to compete in cyberspace as failing to do so will undermine their national power and (cyber)security while empowering their adversaries. Agreed competition, in contrast, is driven not by exploitation but by the will to expand and maximize power to achieve global cyberhegemony, cyberspace’s dominant behaviors. This implies that competitive cyberinteractions may persist under the leadership of a hegemon in cyberspace due to the inherent vulnerabilities, constant contact, and technological volatility of the domain. Answering the

questions raised by cyberdominance consequently remains an empirical challenge.

Acknowledgments

This research article is derived from the author’s doctoral dissertation entitled “Great Power Cyberpolitics: Re-Interpreting Offensive Realism and Power Transition Theory for Cyber Deterrence.” The author would like to thank Prof. Steven Roach for his editorial support, Dr. Nathan Barrick and doctoral student Grant Peeler for their suggestions and writing support, and Prof. Earl Conteh-Morgan, Prof. Nezir Akyesilmen, Dr. Nicolas W. Thompson, Dr. Holly Dunn, Prof. Abdelwahab Hechiche, and the anonymous reviewers for their valuable comments and suggestions. This research was sponsored by the Republic of Türkiye. The author reports that there are no competing interests to declare.

Notes

- 1 Some question the strategic saliency of cyberoperations. Erik Gartzke (2013, 57–58) believes that cyberconflict is neither transformative in modern warfare nor a standalone means of coercion given the problem of attribution and the temporary effects of cyberoperations. Thus, cyberwar can arguably only function as a force multiplier alongside conventional warfare and cannot shift the balance of power (Liff 2012). Similarly, after examining the history of cyberconflict between states that have traditionally been rivals, others have concluded that cybercoercion is limited, as restraint appears to be the norm in interstate cybersecurity relations due to a desire to avoid escalation. However, this trend may change in the future (Craig and Valeriano 2018, 95; Valeriano and Maness 2015).
- 2 John Mearsheimer (2001a) primarily anchored his empirical analysis on US grand strategy.
- 3 One may argue that OR is unfit to explain great power politics in a specific domain of competition; thus, inconsistencies in the behavior of great powers across domains are unsurprising. But OR treats the pursuit of power as the dominant behavior for major states, regardless of domain, because anarchy incentivizes them to expand via power maximization when and where possible (Mearsheimer 2001a, 21–36). Therefore, the approaches major powers adopt for specific domains tend to match their overall strategic frameworks. For instance, economic and technological power ultimately boosts military capabilities: China can hardly challenge the US’s military dominance without economic strength (Tammen 2008, 320). During the Cold War, the superpowers displayed nearly consistent patterns of behavior across military, economic, and ideological domains. Moscow and

Washington competed over outer space (e.g., Russian launch of Sputnik), developed conventional and nuclear capabilities (e.g., ballistic missiles and nuclear-powered submarines), boosted their naval and air capabilities, and pursued ideological dominance (e.g., communism versus capitalism) (Powaski 1997). Yet examples of inconsistent great power behavior across domains exist. The United Kingdom favored naval supremacy over land power to maintain its empire (Kennedy 2017). However, it is one thing to try to maximize power across domains and another to achieve dominance in all of them. Therefore, OR expects great powers to act consistently in pursuing dominance across domains of competition because the logic of power maximization remains constant.

- 4 Scholars also debate whether cyberpower has empowered small states and nonstate actors while eroding the supremacy of major states in IR (Valeriano, Jensen, and Maness 2018, 53–54). Some argue that the proliferation of ICTs has diffused power among cyberactors, empowering weaker states and nonstate entities (Choucri and Clark 2018, 356). For example, Iran cannot defeat the US in a conventional war given the latter's unrivaled military capability, but it can challenge Washington in cyberspace, as it is less wired and is thus less vulnerable to cyberthreats. However, critics reject this as "technological determinism." While accepting that cyberpower is more diffused, they argue that there is a limit to how much cyberpower small states and nonstate actors can produce. The incomparable resources of great powers (rooted, for example, in their control of large geographical areas) grant them supremacy in leveraging cybercapabilities and cyberviolence. Consequently, the new domain has not leveled the playing field by empowering small states and nonstate actors at the expense of the great powers (Nye 2011, 121–23; Valeriano and Maness 2017, 261–62).
- 5 For conceptual clarity, cyberconflict differs analytically from cybercompetition, especially in duration and intensity. Cybercompetition involves iterative and often covert activities (e.g., intelligence gathering) to gain strategic advantages, and can shift the interstate balance of (cyber)power in the long term without escalation to a wider conflict (Harknett and Smeets 2022, 535–38). Cyberconflict can also shift power dynamics, but usually in the short term. Unlike competitive cyberengagements, cyberconflict entails more aggressive actions, including degradation and destruction (Valeriano, Jensen, and Maness 2018, 36–41, Valeriano and Meness 2015, 21). Yet this conceptual distinction may be subtle and elusive due to some overlaps in objectives and tactics. For example, cyberconflict also includes low-intensity cyberactivities such as spying (Healey 2013, 15).
- 6 Another major debate concerns whether cyberconflict is coercive. Critics highlight the absence of physical violence and human casualties from cyberconflicts, the temporary effects of cyberoperations, and the rarity of cybercoercion in cyberincidents (Craig and Valeriano 2018, 89–93; Gartzke 2013, 57–58; Harknett and Smeets 2022, 538; Rid 2012; Valeriano and Maness 2015). However, counterarguments suggest that states can face existential threats in cyberwars, as these conflicts can cause physical destruction and serve as a tool of coercion to extract political concessions (Clarke and Knake 2010; Liff 2012, 403–4). Although these counterarguments may appear speculative, the cases of Stuxnet and the Ukraine blackout provide them with empirical backing, illustrating the strategic, political, coercive, and destructive dimensions of cyberconflict (Akdağ 2017, 115–20; Buchanan 2016, 190; Farwell and Rohozinski 2011, 24).
- 7 However, Christopher Layne (2006) challenges this observation by arguing that the US has indeed pursued a global hegemony that has entailed costly commitments across regions.
- 8 However, it remains unclear if this dominance has been achieved through differences in cyberpower or through the US's unrivaled kinetic power advantage (Valeriano, Jensen, and Maness 2018, 82).
- 9 A similar point has also been made by CPT scholars (Fischerkeller, Goldman, and Harknett 2022, 30–36).
- 10 While some scholars define cyberspace as anarchic due to its decentralized nature, others disagree (Choucri 2012, 43; Craig and Valeriano 2018, 88; Lindsay 2017, 495–96). An integrated framework of "hierarchy in anarchy" to describe the political structure of cyberspace reconciles this divergence (Akdağ 2023).
- 11 However, OR faces criticism for ignoring nonsystemic variables (e.g., nonstate actors) in its explanatory framework, and for its pessimistic predictions about China's rise (Jung and Lee 2017, 86–87; Kirshner 2012, 51; Snyder 2002, 171–72; Toft 2005, 393). Layne (2006) criticizes Mearsheimer for overrating the effect of geographical constraints on the expansionist behavior of great powers. Layne argues that natural barriers have neither stopped Washington's projection of extraregional power nor transformed the US from a power maximizer into a status quo-seeking regional hegemon. Rather, the US sought global hegemony in the post-World War II order, as indicated by its declaratory policies and actions.
- 12 The indicators Layne (2006) uses to test Mearsheimer's prediction about expansion inspired this analysis.
- 13 This point is contestable, as Stuxnet inflicted temporary damage on Iranian nuclear infrastructure and only had a transient effect (Valeriano, Jensen, and Maness 2018, 40–41).

14 Interestingly, CPT scholars do not conceptualize cybepower, but rather mention general balance-of-power or strategic advantages (Fischerkeller, Goldman, and Harknett 2022).

References

- Akdağ, Yavuz. 2017. "Cyber Deterrence against Cyberwar between the United States and China: A Power Transition Theory Perspective." Master's thesis. University of South Florida. <https://digitalcommons.usf.edu/etd/6993>.
- . 2019. "The Likelihood of Cyberwar between the United States and China: A Neorealism and Power Transition Theory Perspective." *Chinese Journal of Political Science* 24 (2): 225–47. DOI: 10.1007/s11366-018-9565-4.
- . 2023. "Great Power Cyberpolitics: Re-Interpreting Offensive Realism and Power Transition Theory for Cyber Deterrence." PhD diss. University of South Florida. <https://digitalcommons.usf.edu/etd/10017>.
- Arquilla, John, and David Ronfeldt. 1997. "Cyberwar Is Coming!" In *Athena's Camp: Preparing for Conflict in the Information Age*, eds. John Arquilla and David Ronfeldt, 23–60. Santa Monica, CA: RAND Corporation.
- Betz, David J., and Tim Stevens. 2011. "Endnotes." In *Cyberspace and the State: Toward a Strategy for Cyber-Power. Adelphi Series* 51 (424): 141–58. DOI: 10.1080/19445571.2011.636959.
- Brandes, Sean. 2013. "The Newest Warfighting Domain: Cyberspace." *Synesis: A Journal of Science, Technology, Ethics, Policy* 4: 90–95. http://synesisjournal.com/vol4_g/Brandes_2013_G90-95.pdf.
- Brantly, Aaron F. 2018. "The Cyber Deterrence Problem." In 2018 *10th International Conference on Cyber Conflict. CyCon X: Maximising Effects*, eds. Tomáš Minárik, Raik Jakschis, and Lauri Lindström, 31–54. New York: Institute of Electrical and Electronics Engineers. DOI: 10.23919/CYCON.2018.8405009.
- Borger, Julian. 2013. "NSA Files: What's a Little Spying between Old Friends?" *Guardian*, December 2. <https://www.theguardian.com/world/2013/dec/02/nsa-files-spying-allies-enemies-five-eyes-g8>.
- Brooks, Stephen G., and William C. Wohlforth. 2008. *World out of Balance: International Relations and the Challenge of American Primacy*. Princeton, NJ: Princeton University Press. DOI: 10.1515/9781400837601.
- Buchanan, Ben. 2016. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. Oxford: Oxford University Press. DOI: 10.1093/acprof:oso/9780190665012.001.0001.
- Cavelty, Myriam Dunn. 2018. "Europe's Cyber-Power." *European Politics and Society* 19 (3): 304–20. DOI: 10.1080/23745118.2018.1430718.

- Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press. DOI: 10.7551/mitpress/7736.001.0001.
- Choucri, Nazli, and David D. Clark. 2018. *International Relations in the Cyber Age: The Co-Evolution Dilemma*. Cambridge, MA: MIT Press. DOI: 10.7551/mitpress/11334.001.0001.
- Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: HarperCollins.
- Craig, Anthony, and Brandon Valeriano. 2016. "Conceptualising Cyber Arms Races." In 2016 *8th International Conference on Cyber Conflict (CyCon): Cyber Power*, eds. Nikolaos Pissanidis, Henry Róigas, and Matthijs Veenendaal, 141–58. New York: Institute of Electrical and Electronics Engineers. DOI: 10.1109/CYCON.2016.7529432.
- . 2018. "Realism and Cyber Conflict: Security in the Digital Age." In *Realism in Practice: An Appraisal*, eds. Davide Orsi, J. R. Avgustin, and Max Nurnus, 85–101. Bristol: E-International Relations.
- DeVore, Marc R., and Sangho Lee. 2017. "APT (Advanced Persistent Threats) and Influence: Cyber Weapons and the Changing Calculus of Conflict." *Journal of East Asian Affairs*: 39–64. <https://www.jstor.org/stable/44321272>.
- Ebert, Hannes, and Tim Maurer. 2013. "Contested Cyberspace and Rising Powers." *Third World Quarterly* 34 (6): 1054–74. DOI: 10.1080/01436597.2013.802502.
- Farwell, James P., and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival* 53 (1): 23–40. DOI: 10.1080/00396338.2011.555586.
- Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2022. *Cyber Persistence Theory: Redefining National Security in Cyberspace*. Oxford: Oxford University Press. DOI: 10.1093/oso/9780197638255.001.0001.
- Fischerkeller, Michael P., and Richard J. Harknett. 2019. "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation." *Cyber Defense Review* (special edition): 267–87. https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf.
- Gao, Xinchuchu. 2022. "An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model." *International Spectator* 57 (3): 15–30. DOI: 10.1080/03932729.2022.2074710.
- Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth." *International Security* 38 (2): 41–73. DOI: 10.1162/ISEC_a_00136.
- Gartzke, Erik, and Jon R. Lindsay. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24 (2): 316–48. DOI: 10.1080/09636412.2015.1038188.

- Gorwa, Robert, and Max Smeets. 2019. "Cyber Conflict in Political Science: A Review of Methods and Literature." Working paper prepared for the 2019 International Studies Association Annual Convention, July 25. OSF preprint. DOI: [10.31235/osf.io/fc6sg](https://doi.org/10.31235/osf.io/fc6sg).
- Haizler, Omry. 2017. "The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking." *Cyber, Intelligence, and Security* 1 (1): 31–45. <https://www.inss.org.il/wp-content/uploads/2017/03/The-United-States%E2%80%99-Cyber-Warfare-History-Implications-on.pdf>.
- Harknett, Richard J., and Max Smeets. 2022. "Cyber Campaigns and Strategic Outcomes." *Journal of Strategic Studies* 45 (4): 534–67. DOI: [10.1080/01402390.2020.1732354](https://doi.org/10.1080/01402390.2020.1732354).
- Harold, Scott W., Martin C. Libicki, and Astrid Stuth Cevallos. 2016. "The 'Cyber Problem' in US–China Relations." In *Getting to Yes with China in Cyberspace*, eds. Scott W. Harold, Martin C. Libicki, and Astrid Stuth Cevallos, 1–16. Santa Monica, CA: RAND Corporation. <https://www.jstor.org/stable/10.7249/j.ctt1cx3vfr.6>.
- Healey, Jason. 2013. "A Brief History of U.S. Cyber Conflict." In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, ed. Jason Healey, 14–87. Vienna, VA: Cyber Conflict Studies Association.
- . 2019. "The Implications of Persistent (and Permanent) Engagement in Cyberspace." *Journal of Cybersecurity* 5 (1): 1–15. DOI: [10.1093/cybsec/tyz008](https://doi.org/10.1093/cybsec/tyz008).
- Healey, Jason, and Robert Jarvis. 2020. "The Escalation Inversion and Other Oddities of Situational Cyber Stability." *Texas National Security Review* 3 (4): 30–53. DOI: [10.26153/tsw/10962](https://doi.org/10.26153/tsw/10962).
- Hill, Richard. 2014. "The Internet, Its Governance, and the Multi-Stakeholder Model." *Info* 16 (2): 16–46. DOI: [10.1108/info-05-2013-0031](https://doi.org/10.1108/info-05-2013-0031).
- Inkster, Nigel. 2014. "The Snowden Revelations: Myths and Misapprehensions." *Survival* 56 (1): 51–60. DOI: [10.1080/00396338.2014.882151](https://doi.org/10.1080/00396338.2014.882151).
- Jenkinson, Andrew. 2021. *Stuxnet to Sunburst: 20 Years of Digital Exploitation and Cyber Warfare*. Boca Raton, FL: CRC Press. DOI: [10.1201/9781003204145](https://doi.org/10.1201/9781003204145).
- Jervis, Robert. 1978. "Cooperation under the Security Dilemma." *World Politics* 30 (2): 167–214. DOI: [10.2307/2009958](https://doi.org/10.2307/2009958).
- Jung, Sung Chul, and Kihyun Lee. 2017. "The Offensive Realists Are Not Wrong: China's Growth and Aggression, 1976–2001." *Pacific Focus* 32 (1): 86–108. DOI: [10.1111/pafo.12088](https://doi.org/10.1111/pafo.12088).
- Kello, Lucas. 2013. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38 (2): 7–40. DOI: [10.1162/ISEC_a_00138](https://doi.org/10.1162/ISEC_a_00138).
- Kennedy, Paul. 2017. *The Rise and Fall of British Naval Mastery*. London: Penguin.
- Keohane, Robert O. 2020. *International Institutions and State Power: Essays in International Relations Theory*. New York: Routledge. DOI: [10.4324/9780429032967](https://doi.org/10.4324/9780429032967).
- Kesan, Jay P., and Carol M. Hayes. 2012. "Mitigating Counterstriking: Self-Defense and Deterrence in Cyberspace." *Harvard Journal of Law and Technology* 25 (2): 429–543. <https://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech429.pdf>.
- Kirshner, Jonathan. 2012. "The Tragedy of Offensive Realism: Classical Realism and the Rise of China." *European Journal of International Relations* 18 (1): 53–75. DOI: [10.1177/1354066110373949](https://doi.org/10.1177/1354066110373949).
- Klimburg, Alexander. 2011. "Mobilising Cyber Power." *Survival* 53 (1): 41–60. DOI: [10.1080/00396338.2011.555595](https://doi.org/10.1080/00396338.2011.555595).
- . 2020. "Mixed Signals: A Flawed Approach to Cyber Deterrence." *Survival* 62 (1): 107–30. DOI: [10.1080/00396338.2020.1715071](https://doi.org/10.1080/00396338.2020.1715071).
- Landau, Susan. 2013. "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations." *IEEE Security & Privacy* 11 (4): 54–63. DOI: [10.1109/MSP.2013.90](https://doi.org/10.1109/MSP.2013.90).
- Layne, Christopher. 2002. "The 'Poster Child for Offensive Realism': America as a Global Hegemon." *Security Studies* 12 (2): 120–64. DOI: [10.1080/09636410212120011](https://doi.org/10.1080/09636410212120011).
- . 2006. *The Peace of Illusions: American Grand Strategy from 1940 to the Present*. Ithaca, NY: Cornell University Press.
- Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.
- Libicki, Martin. 2019. "For a Baltic Cyberspace Alliance?" In *2019 11th International Conference on Cyber Conflict (CyCon): Silent Battle*, eds. Tomás Minárik, Siim Alatalu, Stefano Biondi, Massimiliano Signoretti, Ihsan Tolga, and Gábor Visky, 1–14. New York: Institute of Electrical and Electronics Engineers. DOI: [10.23919/CYCON.2019.8756758](https://doi.org/10.23919/CYCON.2019.8756758).
- Liff, Adam P. 2012. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35 (3): 401–28. DOI: [10.1080/01402390.2012.663252](https://doi.org/10.1080/01402390.2012.663252).
- Limnell, Jarno. 2017. "Proportional Response to Cyberattacks." *Cyber, Intelligence, and Security* 1 (2): 37–52. <https://www.inss.org.il/wp-content/uploads/2017/06/3-Proportional-Response-to-Cyberattacks.pdf>.
- Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22 (3): 365–404. DOI: [10.1080/09636412.2013.816122](https://doi.org/10.1080/09636412.2013.816122).

- . 2015. "The Impact of China on Cybersecurity: Fiction and Friction." *International Security* 39 (3): 7–47. DOI: [10.1162/ISEC_a_00189](https://doi.org/10.1162/ISEC_a_00189).
- . 2017. "Restrained by Design: The Political Economy of Cybersecurity." *Digital Policy, Regulation and Governance* 19 (6): 493–514. DOI: [10.1108/DPRG-05-2017-0023](https://doi.org/10.1108/DPRG-05-2017-0023).
- Mazzetti, Mark, and Michael S. Schmidt. 2013. "Ex-Worker at C.I.A. Says He Leaked Data on Surveillance." *New York Times*, June 9. <https://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html>.
- Mearsheimer, John J. 2001a. *The Tragedy of Great Power Politics*. New York: W. W. Norton.
- . 2001b. "The Future of the American Pacifier." *Foreign Affairs* 80 (5): 46–61. DOI: [10.2307/20050250](https://doi.org/10.2307/20050250).
- Nye, Joseph S., Jr. 2011. *The Future of Power*. New York: PublicAffairs.
- . 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41 (3): 44–71. DOI: [10.1162/ISEC_a_00266](https://doi.org/10.1162/ISEC_a_00266).
- Obama, Barack. 2009. "Text: Obama's Remarks on Cyber Security." Transcript of a speech delivered in Washington, DC, May 29. *New York Times*, May 29. <https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html>.
- Park, Donghui, and Michael Walstrom. 2017. "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks." *Feature Series, October* 11. Seattle, WA: Henry M. Jackson School of International Studies, University of Washington. <https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks>.
- Pence, Mike. 2018. "Remarks by Vice President Pence at the DHS Cybersecurity Summit." *Transcript of a speech delivered in New York*, July 31. Washington, DC: The White House. <https://trumpwhitehouse.archives.gov/briefings-statements/remarks-vice-president-pence-dhs-cybersecurity-summit>.
- Powaski, Ronald E. 1997. *The Cold War: The United States and the Soviet Union, 1917–1991*. Oxford: Oxford University Press. DOI: [10.1093/oso/9780195078503.001.0001](https://doi.org/10.1093/oso/9780195078503.001.0001).
- Rendall, Matthew. 2006. "Defensive Realism and the Concert of Europe." *Review of International Studies* 32 (3): 523–40. DOI: [10.1017/S0260210506007145](https://doi.org/10.1017/S0260210506007145).
- Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5–32. DOI: [10.1080/01402390.2011.608939](https://doi.org/10.1080/01402390.2011.608939).
- Ripsman, Norrin M., Jeffrey W. Taliaferro, and Steven E. Lobell. 2016. *Neoclassical Realist Theory of International Politics*. New York: Oxford University Press. DOI: [10.1093/acprof:oso/9780199899234.001.0001](https://doi.org/10.1093/acprof:oso/9780199899234.001.0001).
- Russell, Alison Lawlor. 2014. *Cyber Blockades*. Washington, DC: Georgetown University Press. DOI: [10.1353/book35250](https://doi.org/10.1353/book35250).
- Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance." *Contemporary Security Policy* 34 (1): 40–63. DOI: [10.1080/13523260.2013.771031](https://doi.org/10.1080/13523260.2013.771031).
- Sanger, David E. 2012. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Random House.
- Sheldon, John B. 2011. "Deciphering Cyberpower: Strategic Purpose in Peace and War." *Strategic Studies Quarterly* 5 (2): 95–112. <https://www.jstor.org/stable/26270559>.
- Singer, Peter W. 2015. "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons." *Case Western Reserve Journal of International Law* 47: 79–86. <https://scholarlycommons.law.case.edu/jil/vol47/iss1/10>.
- Slayton, Rebecca. 2017. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41 (3): 72–109. DOI: [10.1162/ISEC_a_00267](https://doi.org/10.1162/ISEC_a_00267).
- Snyder, Glenn H. 2002. "Mearsheimer's World—Offensive Realism and the Struggle for Security: A Review Essay." Review of *The Tragedy of Great Power Politics* by John J. Mearsheimer. *International Security* 27 (1): 149–73. DOI: [10.1162/016228802320231253](https://doi.org/10.1162/016228802320231253).
- Soesanto, Stefan, and Max Smeets. 2021. "Cyber Deterrence: The Past, Present, and Future." In *NL ARMS Netherlands Annual Review of Military Studies 2020*, eds. Frans Osinga and Tim Sweijts, 385–400. The Hague: T. M. C. Asser Press. DOI: [10.1007/978-94-6265-419-8_20](https://doi.org/10.1007/978-94-6265-419-8_20).
- Taddeo, Mariarosaria. 2018. "The Limits of Deterrence Theory in Cyberspace." *Philosophy & Technology* 31 (3): 339–55. DOI: [10.1007/s13347-017-0290-2](https://doi.org/10.1007/s13347-017-0290-2).
- Taliaferro, Jeffrey W. 2001. "Security Seeking under Anarchy: Defensive Realism Revisited." *International Security* 25 (3): 128–61. DOI: [10.1162/016228800560543](https://doi.org/10.1162/016228800560543).
- Tammen, Ronald L. 2008. "The Organski Legacy: A Fifty-Year Research Program." *International Interactions* 34 (4): 314–32. DOI: [10.1080/03050620802561769](https://doi.org/10.1080/03050620802561769).
- Toft, Peter. 2005. "John J. Mearsheimer: An Offensive Realist between Geopolitics and Power." *Journal of International Relations and Development* 8 (4): 381–408. DOI: [10.1057/palgrave.jird.1800065](https://doi.org/10.1057/palgrave.jird.1800065).
- Tor, Uri. 2017. "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence." *Journal of Strategic Studies* 40 (1–2): 92–117. DOI: [10.1080/01402390.2015.1115975](https://doi.org/10.1080/01402390.2015.1115975).
- US Cyber Command. 2022. "Cyber 101: Defend Forward and Persistent Engagement." Press release, October 25. US Cyber Command: Fort George

- G. Meade, MD. <https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement>.
- US Department of Defense. 2011. "Department of Defense Strategy for Operating in Cyberspace." *Strategy document*, July. Washington, DC: Department of Defense. <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>.
- . 2015. "The DoD Cyber Strategy." Strategy document, April 17. Washington, DC: Department of Defense. <https://nsarchive.gwu.edu/document/21384-document-25>.
- . 2018. "Summary: Department of Defense Cyber Strategy 2018." *Strategy document*, September 18. Washington, DC: Department of Defense. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
- . 2023. "DOD Releases 2023 Cyber Strategy Summary." *Press release*, September 12. Washington, DC: Department of Defense. <https://www.defense.gov/News/Releases/Release/Article/3523199/dod-releases-2023-cyber-strategy-summary>.
- US Department of State. 2022. "Declaration for the Future of the Internet." *International partnership agreement*, April 28. Washington, DC: US Department of State. <https://www.state.gov/declaration-for-the-future-of-the-internet>.
- Valeriano, Brandon. 2022. "The Failure of Offense/Defense Balance in Cyber Security." *Cyber Defense Review* 7 (3): 91–102. <https://www.jstor.org/stable/48682325>.
- Valeriano, Brandon, Benjamin M. Jensen, and Ryan C. Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press. DOI: 10.1093/oso/9780190618094.001.0001.
- Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press. DOI: 10.1093/acprof:oso/9780190204792.001.0001.
- . 2017. "International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain." In *The Oxford Handbook of International Political Theory*, eds. Chris Brown and Robyn Eckersley, 259–72. Oxford: Oxford University Press. DOI: 10.1093/oxfordhb/9780198746928.013.19.
- Van Evera, Stephen. 1998. "Offense, Defense, and the Causes of War." *International Security* 22 (4): 5–43. DOI: 10.2307/2539239.
- Voo, Julia, Irfan Hemani, and Daniel Cassidy. 2022. "National Cyber Power Index 2022." *Cyber Project report*, September. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School. <https://www.belfercenter.org/publication/national-cyber-power-index-2022>.
- Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Daniel Cassidy, and Anina Schwarzenbach. 2020. "National Cyber Power Index 2020: Methodology and Analytical Considerations." *China Cyber Policy Initiative report*, September. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School. <https://www.belfercenter.org/publication/national-cyber-power-index-2020>.
- Wahl-Jorgensen, Karin, Lucy Bennett, and Gregory Taylor. 2017. "The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates after the Snowden Revelations." *International Journal of Communication* 11: 740–62. <https://orca.cardiff.ac.uk/id/eprint/97854>.
- Walt, Stephen M. 1985. "Alliance Formation and the Balance of World Power." *International Security* 9 (4): 3–43. DOI: 10.2307/2538540.
- Waltz, Kenneth N. 1979. *Theory of International Politics*. Long Grove, IL: Waveland Press.
- . 1981. "The Spread of Nuclear Weapons: More May Be Better." *Adelphi Series* 21 (171): 1–32. DOI: 10.1080/05679328108457394.
- The White House. 2003. "The National Strategy to Secure Cyberspace." *Strategy document*, February. Washington, DC: The White House. <https://apps.dtic.mil/sti/citations/ADA413614>.
- . 2018. "National Cyber Strategy of the United States." *Strategy document*, September. Washington, DC: The White House. <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
- . 2023. "National Cybersecurity Strategy." *Strategy document*, March 1. Washington, DC: The White House. <https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.
- Wilner, Alex S. 2020. "US Cyber Deterrence: Practice Guiding Theory." *Journal of Strategic Studies* 43 (2): 245–80. DOI: 10.1080/01402390.2018.1563779.
- Wilson, Clay. 2004. "Information Warfare and Cyberwar: Capabilities and Related Policy Issues." *Congressional Research Service Report for Congress RL31787*, July 19. Washington, DC: Congressional Research Service. <https://apps.dtic.mil/sti/citations/ADA477185>.
- Whyte, Christopher. 2018. "Dissecting the Digital World: A Review of the Construction and Constitution of Cyber Conflict Research." *International Studies Review* 20 (3): 520–32. DOI: 10.1093/isr/viw013.
- Whyte, Christopher, and Brian Mazanec. 2018. *Understanding Cyber Warfare: Politics, Policy, and*

Strategy, 1st edition. London: Routledge. DOI: [10.4324/9781315636504](https://doi.org/10.4324/9781315636504).
———. 2023. *Understanding Cyber Warfare: Politics, Policy, and Strategy*, 2nd edition. London: Routledge. DOI: [10.4324/9781003246398](https://doi.org/10.4324/9781003246398).

Zook, Matthew, Lomme Devriendt, and Martin Dodge. 2011. "Cyberspatial Proximity Metrics: Reconceptualizing Distance in the Global Urban System." *Journal of Urban Technology* 18 (1): 93–114. DOI: [10.1080/10630732.2011.578411](https://doi.org/10.1080/10630732.2011.578411).