New England Journal of Public Policy

Volume 36
Issue 1 *The Changing Character of War and Peacemaking*
Article 8

6-16-2024

Understanding the Indirect Strategy Moment in Global Affairs

Kumar Ramakrishna
S. Rajaratnam School of International Studies, Nanyang Technological University

Understanding the Indirect Strategy Moment in Global Affairs

Kumar Ramakrishna
S. Rajaratnam School of International Studies, Nanyang Technological University

Abstract

This article argues that policymakers need to better grasp what can best be understood as the "indirect strategy moment" in global affairs. It explains what is meant by indirect strategy in the classical strategic thought, before analyzing how indirect strategy has already been applied in the post-Cold War era. The article will then illustrate how indirect strategy is being applied in the cyber, social media, and telecommunications domains, before arguing that adopting "indirect strategy lenses" appears to be rather important in order to better frame current and ongoing geostrategic developments across a range of issues and domains. A recurring theme is that in this indirect strategy moment, the line between peace and war has been increasingly blurred.

Kumar Ramakrishna is a professor of National Security Studies, the Provost's Chair in National Security Studies, and Dean of the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. *This article represents a substantive reconceptualization and reworking of the author's "Enter the Age of Csywar: Some Reflections on an Emergent Trend,"* New England Journal of Public Policy *34, no. 2 (2022): Article 5, https://scholarworks.umb.edu/nejpp/vol34/iss2/5.*

More than two years after the Russian invasion of Ukraine in February 2022, it seems that the prospect of an end to the fighting remains as dim as ever. More than that, the threat of escalation through the use of nuclear weapons has, worryingly, also emerged.[1] That being said, it is important to note that the current conflagration is somewhat an anomaly in the context of what had transpired over the past decade. Ever since the initial intervention in eastern Ukraine in March 2014 by Russian troops in unmarked uniforms—the so-called "little green men"[2]—most analysts have argued that low-key "hybrid conflict" has been the norm in the long standoff between Moscow and Kyiv. Hybrid conflict broadly refers to the methods and tools used by individual state or non-state actors to pursue their objectives, spanning the conflict continuum from disinformation to cyber war, energy supply disruption, and traditional warfare.[3] Moscow had in fact been engaging in hybrid conflict with Ukraine since the 2014 intervention.[4]

Thus far, it seems clear that Russian president Vladimir Putin's decision to switch to an outright "special military operation" in February 2022 has not yielded the desired outcome of a Ukrainian military and political capitulation. Instead US intelligence assessments in late 2023 suggested that Russia had "lost a staggering 87 percent of the total number of active-duty ground troops it had" before the invasion, as well as "two-thirds of its pre-invasion tanks."[5] Against such a backdrop, it is not far-fetched to imagine that a ceasefire between Kyiv and Moscow might eventually ensue. Putin may then revert to his previous and relatively far more cost-effective hybrid warfare playbook as the main means to secure his geopolitical objectives vis-à-vis Kyiv.[6] In fact, while NATO governments warned in January 2024 of a possible Russian military attack in five to eight years, in the lead up to such an outcome, NATO remains fully cognizant that the Russian Federation is unlikely to shy away from targeting NATO member states with "sophisticated hybrid strategies, including political interference, malicious cyber activities, economic pressure and coercion, subversion, aggression and annexation" as well as "coercive military posture and rhetoric."[7] Hybrid warfare thus remains highly relevant. More fundamentally, it points to the importance of indirect strategy in global geostrategic competition.

This article develops its argument in the following fashion. It will first briefly explain what is meant by "indirect strategy" in the classical strategic thought. This will be followed by an analysis of how indirect strategy has already been applied in the post-Cold War era. The article will then further examine how indirect strategy has been applied in the cyber, social media, and telecommunications domains, before ending off with a concise analysis as to why adopting "indirect strategy lenses" appears to be rather important in order to better frame current and ongoing geostrategic developments across a range of issues and domains, from economic and technological de-risking to the preservation of domestic socio-political cohesion in the face of foreign influence campaigns by hostile state actors. A recurring theme, as we shall see, is that in this indirect strategy moment, the line between peace and war has been increasingly blurred.

Indirect Strategy Explained

In his classic *Introduction to Strategy* (1963), the French military strategist Andre Beaufre (1902–1975) argued that in the direct mode of warfare, military force plays the decisive role; in the indirect mode, military force plays a secondary role. The theory and practice of indirect strategy is not new. The fifth-century BCE Chinese strategist Sun Tzu emphasized the importance of avoiding the enemy's strengths and attacking his weaknesses instead.[8] The best strategy, according to Sun Tzu, was to "win without fighting."[9] In other words, the ability of a state to

impose its will on the adversary without relying excessively on military power represented the "acme of skill."[10] This basic concept of avoiding adversary strength and attacking his weakness represents the essence of indirect strategy.

The US military acronym DIME—diplomatic, informational, military, and economic elements of state power—helps illustrate the point.[11] If a state decides upon a direct application of DIME, then the military instrument would be preponderant, with the other instruments in support. Conversely, in an indirect application of DIME, the non-kinetic instruments—diplomatic, economic, and informational—would be preponderant in the total strategic response, with the military instrument playing a calibrated supporting role.

Indirect Strategy in the Post-Cold War Era

Beaufre observed that in the Cold War (1945–1990) environment of mutual nuclear deterrence between the superpowers, indirect strategy was very important and "not the direct strategy's adoption of material force."[12] In the post-Cold War era, the continuing imperative to avoid outright confrontation between nuclear-capable great powers, and the understandable reluctance of major peer-competitors of the US to directly engage the latter militarily on the conventional front, has resulted in strategic innovation that prioritizes indirect strategy. Hence, in his book *Battlegrounds,* H. R. McMaster argues that Russia has—since the breakup of the Soviet Union—engaged in so-called hybrid "new-generation warfare" that seeks to avoid direct military confrontation with the West, seeking instead to "disrupt, divide and weaken societies" regarded as competitors.[13] In essence, Russian strategists, declaring that the very "rules of war" have evolved, noted that nonmilitary instruments of achieving political and strategic objectives have grown and, in many cases, have exceeded military force in their effectiveness.[14] Chinese military strategists have similarly argued that modern warfare has evolved and now involves "using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests," and that the many "new battlefields" could include environmental, financial, trade, cultural and legal forms of warfare.[15] Russian and Chinese thinking share the core idea of avoiding Western military strengths and attacking its weaknesses—the essence of indirect strategy.

Indirect Strategy Today

At the current time, indirect strategy is being applied in the cyber, social media, and telecommunications domains, among others.

Cyber Domain

John Carlin in *Dawn of the Code War* observes that the expansion of internet connectivity has rendered national critical infrastructure—water, electricity, communications, and banking—as well as our private information more vulnerable.[16] One result: hostile state actors could mount devastating cyberattacks on a target state's vulnerable, digitally interconnected homeland and cripple it, while bypassing the massed strength of the latter's conventional armed forces. For instance, when Russian forces invaded the Republic of Georgia in 2008, Georgian websites were hit by botnet-mounted distributed denial-of-service (DDoS) attacks in one of the earliest examples of hybrid warfare.[17] This massive cyberattack not only disrupted key government websites, it deprived the Georgian authorities of the ability to communicate with the outside world.[18] To be sure, cyberattacks have been used by all sides for years now. For instance, in December 2023,

Iran's oil minister blamed "outside interference" for disrupting seventy percent of the country's approximately 33,000 gas stations nationwide. The minister added that while 1,650 stations remained operational, others were "forced to operate their pumps manually."[19] An Israel-linked hacker collective called Predatory Sparrow claimed responsibility for the cyberattack, which was in retaliation for Iranian support of Hamas and other militant groups in the context of the current Israel-Hamas war in Gaza following the October 7, 2023 Hamas mass-casualty terror attacks in Israel.[20]

Social Media Space

Meanwhile, as Jacob Helberg asserts in *The Wires of War*, another way that a hostile state may seek to sidestep the military forces of a target state and target the latter's weaker spots, is via intervening in the latter's national social media space. Helberg calls this the "front-end battle," whereby foreign governments attempt to "shape what we think and feel by manipulating the information we consume."[21] While during the Cold War both the United States and the Soviet Union attempted to use media ranging from leaflets to radio broadcasts to shape perceptions in each other's geographical spheres of influence, as Helberg points out, social media has "dramatically transformed the front-end war," deluging audiences with a flood of information, making the distinction between truth and falsehood "infinitely harder to assess."[22] For their part, Peter W. Singer and Emerson T. Brooking likewise warn in their book *LikeWar* that a hostile state, by learning how to manipulate opinion within the target state, can foster "political and social polarization" in the latter—again without a shot being fired—in other words, a classic indirect strategic move.[23] In fact Singer and Josh Baughman argue that the Chinese People's Liberation Army regards so-called "cognitive warfare" to be "on par with the other domains of warfare like air, sea, and space," and Chinese planners believe this indirect strategic maneuver to be the "key to victory—particularly victory without war."[24] They point to Chinese influence operations increasingly using AI where machine learning is employed to "mine user emotions and prejudices to screen and target the most susceptible audiences, and then quickly and intensively 'shoot' customized 'spiritual ammunition' to the target group."[25] The overall aim is to is to weaken the target state indirectly by exploiting its social media space to "'fuel the flames' of existing biases and manipulate emotional psychology to influence and deepen a desired narrative" that serves the interests of the hostile, intervening state.[26] As in the cyber domain, deliberate influence operations that seek to manipulate the national social media space of a target state is increasingly commonplace. For instance, it is now known that former US president Donald Trump directed the Central Intelligence Agency to "launch a clandestine campaign on Chinese social media" led by a "small team of operatives who used bogus internet identities to spread negative narratives" about Beijing while deliberately "leaking disparaging intelligence to overseas news outlets."[27]

Telecommunications Domain

One of the ongoing criticisms of the widely popular social media app TikTok is that under Chinese national security laws, Chinese big tech firms like ByteDance, which owns TikTok, are obligated to, if so required, ensure that user data—even that of citizens of other countries—is made available to Beijing, despite privacy concerns.[28] For instance, it was found out that China-based employees of ByteDance have been able to repeatedly access private data about US TikTok users, prompting former president Trump to threaten to ban the app in the United States.[29] Ultimately, despite TikTok's public assurances that it is making the effort to "cordon off access to the most sensitive

details about Americans that exist on TikTok's servers," it has been acknowledged that in the final analysis, it's their system, as the underlying telecommunications architecture is built in China.[30] In a wider sense, it is notable that China has also begun to seek greater influence over the future versions of the internet, with a view to shaping its development as a means of commerce, communications, and even conflict.[31] This is highly significant from an indirect strategy vantage point, because as Helberg argues pithily, by capturing control of the core layer of the Internet, "you control everything" and can therefore more readily bypass the massed armed strength of the target state, and instead, attack its societal soft underbelly.[32]

In this respect, China's not often obvious quest to dominate the backend architecture of the internet is noteworthy. By 2020, the leading telecommunications firm Huawei dominated about 30 percent of the global market share in telecommunications equipment, while making significant progress toward the goal of capturing the emerging market in fifth-generation communications networks.[33] These networks, known as 5G, which are a hundred times faster than 4G in speed of information transfer, are potentially transformative in the context of the rapidly emerging global internet of things—"the vaguely defined network of millions of internet-linked devices."[34] From an indirect strategic perspective, dominating the lucrative 5G market confers huge advantages: a hostile-state linked telecommunications firm that builds and runs a nation's 5G network will have little trouble, according to Robert Spalding, "stealing and mining all the data on that network: all the academic papers and research, all engineering and business plans, all the photos, emails, and text messages."[35] Additionally, if needed, a hostile state could, through such indirect control of a target state's 5G network, potentially not merely access, but delete and manipulate data as well.[36] More ominously, some analysts warn that in a conflict, a hostile state could even "weaponize" the 5G technology managed by an affiliated network by, for instance, directing self-driving cars into crowds or flying drones into the flight path of commercial aircraft.[37]

That being said, a sense of perspective is in order, as not all countries are ready for the mass adoption of 5G technology. For instance, analysts argue that Southeast Asia is not likely to become an important global market for 5G in the short to medium term.[38] Moreover, while some states like Malaysia allowed Huawei to participate in its 5G rollout, Vietnam opted to develop its own 5G technology, and Singapore granted 5G contracts to Nokia and Ericsson. While Indonesia has been open to buying Chinese telecom equipment, partly due to its relatively low cost and support for capability development, Indonesian cybersecurity officials are aware of the possible risks associated with its use."[39] The upshot of the preceding analysis of indirect strategy in the strategic telecommunications domain is simple. Data, as Helberg argues, can arguably be seen as the "new oil" and information the "most contested geopolitical resource" sought after by many states.[40] He states that "the strategic significance of data and information is increasingly stretching beyond the realm of intelligence collection and into the realm of political influence and control."[41]

At a more fundamental level, this discussion of indirect strategy as operationalized in the cyber, social media, and telecommunications spheres, shows one way that the line between war and peace in contemporary warfare is increasingly blurred.[42]

Adopting Analytical Lenses Appropriate for Navigating the Indirect Strategy Moment in Global Affairs

A key implication of the foregoing analysis is that adopting "indirect strategy lenses" appears to be rather important in order to frame current and ongoing geostrategic developments across a range of issues and domains.

De-risking Viewed Through an Indirect Strategy Lens

A first set of lenses relates to the increasingly pertinent issue of economic and security *de-coupling* or *de-risking*. Simply put, de-coupling, the older term, suggests a "radical separation," while de-risking, which was coined in the financial sector, essentially means "curbing risks while avoiding a clean break."[43] In the context of US-China geopolitical competition, practitioners and analysts have recently argued that full de-coupling from China would be highly impractical, as it is the world's largest manufacturer of goods and the biggest trading partner of a majority of countries. Beijing would thus have the edge if other countries were forced to pick sides. In any case, current economic interlinkages between the US and China may actually serve as a check on Chinese global unilateralism. Hence, the more modest notion of selective de-risking has been increasingly mooted.[44] From my perspective, quite apart from the arguments for economic, technological, and security self-reliance, de-risking is arguably also another way in which countries could seek to indirectly weaken the national capabilities and potentials of peer-competitors without recourse to costly armed conflict. This can be illustrated in the case of semiconductors and rare earth metals.

Semiconductors

Much has been made of US-Chinese strategic competition for control of the manufacturing supply chains for semiconductors and high-performing microchips that are critical for everything from artificial intelligence to cell phones.[45] From an indirect strategy perspective, a state that is able to dominate the global supply chain for such critical chips would be able to indirectly weaken a peer-competitor's national capabilities. This is likely one factor why in mid-2023, at the urging of the US, the Netherlands—where ASML, a leading manufacturer of chipmaking machinery resides—imposed export restrictions on such technology, a move that analysts argue targets China.[46] ASML produces equipment that is used by the Taiwan Semiconductor Manufacturing Company Limited (TSMC),[47] the Taiwanese firm that produces an estimated 90 percent of the world's highly advanced semiconductors and supplies global technology giants like Apple and Nvidia. Significantly, TSMC has also invested in a second semiconductor plant in the US state of Arizona, in addition to one in Japan under its subsidiary the Japan Advanced Semiconductor Manufacturing, Inc. (JASM).[48] In addition, the US passed the CHIPS and Science Act in August 2022, which authorizes fifty-two billion USD to boost domestic semiconductor manufacturing.[49] The bottom line? Washington appears to be coordinating with its allies and partners to ensure that China—whose own semiconductor industry is significantly less advanced—would be unable to dominate this vital global industry.[50]

Rare Earth Metals

Indirect strategy lenses are also helpful in analyzing developments in the equally important domain of rare earth metals. If China is lagging behind in semiconductor manufacturing, it is a different story in the rare earth metals case. To illustrate, China produces 80 percent of the world's gallium and 60 percent of germanium, which are needed to produce chips and significantly, have military applications.[51] In July 2023, in response to the imposition of chip technology export restrictions by the US, Japan, and the Netherlands, Beijing announced curbs on the export of gallium and germanium. As one analyst argued, China's posture was a case of "if you won't give us chips, we won't give you the materials to make those chips."[52] To be sure, China "accounts for 63 percent of the world's rare earth mining, 85 percent of rare earth processing, and 92 percent of rare earth magnet production."[53] Such rare earth alloys and magnets that China produces are crucial components in firearms, missiles, radars, and stealth aircraft.[54] US military night vision goggles

also require Chinese specialty metals as a critical component.[55] Furthermore, China remains the "only country in the world that's developed the capacity to cover the entire value chain of 17 rare earth elements" and has "developed the advantages in not just technology, but also waste management."[56] Chinese technical advantages in and ensuing domination of the global supply chain for rare earth metals, in short, is another illustration of how a state could indirectly weaken the national capabilities of its peer-competitors without recourse to costly armed conflict. In sum, a state that dominates strategically critical supply chains and resources—while systematically and deliberately denying such advantages to peer-competitor states—can gradually impose its geopolitical will and undermine its adversaries without the need for direct military confrontation, another example of the indirect strategic emphasis on avoiding adversary strength and targeting its weaknesses instead.

Indirect Strategy Across the Hybrid Conflict Spectrum

It is important to reiterate the earlier point that indirect strategy lenses are important if we are to make sense of how the line between peace and war has increasingly been blurred. Examples abound, if one were to just observe carefully. For example, experts allege that Chinese maritime vessels have been deliberately cutting underwater internet cables linking the Matsu islands to the main island of Taiwan, to compromise the latter's internal communications connectivity—a crucial requirement for the island's national security, and a shrewd example of a hybrid, indirect approach.[57] As another example, Russia, the world's biggest wheat exporter, could weaponize food exports to undermine its wheat-dependent strategic competitors if it should decide to.[58] Once again: the essence of indirect strategy is to avoid adversary strength and target his weaknesses instead.

In the case of Southeast Asia, moreover, Chinese state-backed hackers have been reported to be "incredibly active" in targeting government and military targets in member states of the Association of Southeast Asian Nations (ASEAN), and have "quietly compromised" them by exfiltrating sensitive information.[59] It was reported that in 2023 that a Chinese hacker collective called Stately Taurus "compromised a Philippine government agency for five days," around the same time as "clashes between the two countries' ships in the South China Sea."[60] That the Philippines has a "soft underbelly" in its cyber sector is attested to by the fact that more than 60,000 user accounts were compromised in the third quarter of 2023, meaning that the Philippines was "among the world's thirty most-attacked countries."[61] Philippine officials have bemoaned the fact that they lack sufficient numbers of "cyber warriors" to shore up this vulnerable sector, thereby inviting indirect approaches by hostile state actors that seek to avoiding Manila's military strengths and to exploit its cyber weaknesses instead.[62]

It cannot be overstated that indirect strategy lenses are vitally useful in helping states anticipate how hostile actors could seek to undermine them from within by disrupting social and political cohesion. Observers have noted that Russian state-backed social media manipulation of socio-political fault-lines within neighboring states have included the exploitation of ethnic tensions and historical revisionism in Estonia, culture and religion in Georgia, political polarization in Poland, and anti-migrant sentiment in the Czech Republic.[63] In 2023, the New Zealand government warned publicly about the "targeting" of its "diverse ethnic Chinese communities by groups and individuals linked to China's intelligence arm."[64] Incidentally, Singapore, where the current writer hails from, shares with New Zealand concerns about foreign influence operations. It is no secret that militarily the well-trained and well-equipped Singapore Armed Forces have a well-established reputation as a potent deterrent against direct military aggression.[65] Hence, in this indirect strategy moment, potential adversaries would likely explore more cost-

effective, indirect, hybrid approaches to shrewdly and subtly impose their will upon globalized, multicultural states like Singapore, even during peacetime. One way would certainly be through foreign influence operations aimed at spreading disinformation, false narratives, and outright falsehoods to undermine trust between Singaporeans and their government.

It is little wonder that the Singaporean government in recent years has tried to shore up domestic socio-political cohesion through legislation such as the Protection from Online Falsehoods and Manipulation Act 2019 (POFMA). Passed in June 2019, POFMA "helps protect the Singapore public against online harm by countering the proliferation of online falsehoods," through "correction directions which require recipients to insert a notice against the original post, with a link to the Government's clarification."[66] The idea is that the "clarification sets out the falsehoods and facts for the public to examine, without the original post being removed," so that readers "can read both the original post and the facts, and decide for themselves what is the truth."[67] More recently, under the newer Foreign Interference (Countermeasures) Act 2021 (FICA), Singaporean individuals delivering speeches, interviews, or written articles that promote the political interests of a foreign entity would be legally required to "make yearly disclosures to the authorities of political donations of $10,000 or more that he has received and accepted, and declare his foreign affiliations and any migration benefits."[68] The rationale behind the relatively calibrated FICA law is to send the signal that Singapore remains open to foreign business—but not foreign interference.[69]

Concluding Observations

Singapore is world-renowned for being a highly cosmopolitan, religiously and culturally diverse, and stable society.[70] Yet a scan of the angry statements circulated on social media platforms frequented by Singaporeans in the wake of the outbreak of the highly destructive Israel-Hamas conflict in Gaza, suggests that domestic socio-political fault-lines remain a potential weakness that hostile state actors or even transnational terrorist groups could exploit via indirect means, through orchestrated social media campaigns. [71] This is precisely why analyst Ajit Mann is correct in reminding us more generally that "dominating the narrative space should be a national security priority," as that is where "non-state actors fight best" and "foreign governments have proven effective in waging war against us without implementing kinetic force."[72]

In the final analysis, in this indirect strategy moment in global affairs, states need to conceive of far more than merely kinetic threats. As this article has suggested, while some state actors may prioritize armed force to attain their objectives—such as Russia in the case of Ukraine since February 2022—more often than not, the indirect strategic approach of avoiding target state strength and attacking its weaknesses is increasingly being adopted, whether one thinks about Russian new-generation warfare or the Chinese "three warfares"—public opinion warfare, psychological warfare, and legal warfare.[73] In fact, it is clear that many other states, including the US, have become more aware of the indirect strategic approach and have at times adopted it themselves, ranging from influence operations to economic, technological de-risking aimed at undermining the longer-term national capabilities of peer-competitors. In this era of hybrid conflict and indirect strategy, as Sean McFate argues, there is increasingly "no such thing as war or peace – both co-exist, always."[74] It thus behooves national security practitioners, analysts and even the general public, to better grasp how their nation-states could be shrewdly undermined by subtle, not immediately obvious, non-kinetic, indirect strategic approaches. In this indirect strategy moment in global affairs, in short, as the old saying goes: "You may not be interested in war, but war is interested in you."[75]

Notes

[1] Guy Faulconbridge and Lidia Kelly, "Putin Warns the West: Russia Is Ready for Nuclear War," *Reuters*, March 14, 2024, https://www.reuters.com/world/europe/putin-says-russia-ready-nuclear-war-not-everything-rushing-it-2024-03-13/.
[2] Vitaly Shevchenko, "'Little Green Men' or 'Russian Invaders'?," *BBC News*, March 11, 2024, https://www.bbc.com/news/world-europe-26532154.
[3] Tarik Solmaz, "'Hybrid Warfare': One Word, Many Meanings," *Small Wars Journal*, February 25, 2022, https://smallwarsjournal.com/jrnl/art/hybrid-warfare-one-term-many-meanings.
[4] David Kilcullen, "Russia's War in Ukraine Is Complex and Probably Underway," *UNSW Newsroom*, February 4, 2022, https://www.unsw.edu.au/newsroom/news/2022/02/russia-s-war-in-the-ukraine-is-complex-and-probably-already-unde.
[5] Katie Bo Lillis, "Russia Has Lost 87% of Troops It Had Prior to Start of Ukraine War, according to US Intelligence Assessment," *CNN*, December 13, 2023, https://amp-cnn-com.cdn.ampproject.org/c/s/amp.cnn.com/cnn/2023/12/12/politics/russia-troop-losses-us-intelligence-assessment/index.html.
[6] Mason Clark, "Russian Hybrid Warfare," *Institute for the Study of War*, September 2020, https://www.understandingwar.org/report/russian-hybrid-warfare.
[7] Nicholas Camut, "Putin Could Attack NATO in '5 to 8 Years,' German Defense Minister Warns," *Politico*, January 19, 2024, https://www.politico.eu/article/vladimir-putin-russia-germany-boris-pistorius-nato; "Countering Hybrid Threats," *North Atlantic Treaty Organization*, March 7, 2024, https://www.nato.int/cps/en/natohq/topics_156338.htm.
[8] Mark R. McNeilly, *Sun Tzu and the Art of Modern Warfare* (New York: Oxford University Press, 2015).
[9] Ibid.
[10] "Sun Tzu, c. 400–320 BC, Chinese General and Military Theorist," in *Oxford Essential Quotations*, 5th ed., ed. Susan Ratcliffe (New York: Oxford University Press, 2017), https://www.oxfordreference.com/display/10.1093/acref/9780191866692.001.0001/q-oro-ed6-00010536;jsessionid=A8B662CCA1AC9B0F64BD7BADAD9E5E02.
[11] Steven Aftergood, "Strategy: Directing the Instruments of National Power," *Federation of American Scientists*, April 30, 2018, https://fas.org/publication/strategy-jcs/.
[12] Tim Kumpe, "Andre Beaufre in Contemporary Chinese Strategic Thinking," *Military Strategy Magazine* 5, no. 2 (Spring 2016), https://www.militarystrategymagazine.com/article/andre-beaufre-in-contemporary-chinese-strategic-thinking/.
[13] H. R. McMaster, *Battlegrounds: The Fight to Defend the Free World* (New York: Harper, 2020), 40–41.
[14] Molly K. McKew, "The Gerasimov Doctrine: It's Russia's New Chaos Doctrine of Political Warfare. And It's Probably Being Used on You," *Politico*, September/October 2017, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/.
[15] David Barno and Nora Bensahel, "A New Generation of Unrestricted Warfare," *War on the Rocks*, April 19, 2016, https://warontherocks.com/2016/04/a-new-generation-of-unrestricted-warfare/.
[16] John P. Carlin, with Garrett M. Graff, *Dawn of the Code War: America's Battle against Russia, China and the Rising Global Cyber Threat* (New York: Public Affairs, 2018), 42.
[17] Ibid., 158.
[18] Nina Jankowicz, *How to Lose the Information War: Russia, Fake News, and the Future of Conflict* (London: I. B. Tauris, 2020), 60–61.
[19] Daryna Antoniuk, "Iran Confirms Nationwide Cyberattack on Gas Stations," *The Record*, December 19, 2023, https://therecord.media/iran-cyberattack-gas-stations-israel.
[20] Ibid.
[21] Jacob Helberg, *The Wires of War: Technology and the Global Struggle for Power* (New York: Avid Reader Press, 2021), 52.
[22] Ibid., 52–53.
[23] P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt, 2018), 126–27.
[24] Josh Baughman and Peter W. Singer, "China's Social-Media Attacks Are Part of a Larger 'Cognitive Warfare' Campaign," *Defense One*, October 17, 2023, https://www.defenseone.com/ideas/2023/10/chinas-social-media-attacks-are-part-larger-cognitive-warfare-campaign/391255/?oref=defense_one_breaking_nl.

[25] Ibid.
[26] Ibid.
[27] "Trump Launched Covert Influence Operation against China," *CNA*, March 15, 2024, https://www.channelnewsasia.com/world/former-us-president-donald-trump-launched-covert-cia-influence-operation-against-china-4197016.
[28] Emily Baker-White, "Leaked Audio from 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed from China," *BuzzFeed News*, June 18, 2022, https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access.
[29] Ibid.
[30] Ibid.
[31] Baughman and Singer, "China's Social-Media Attacks."
[32] Helberg, *Wires of War*, 145.
[33] McMaster, *Battlegrounds*, 141.
[34] Bill Geertz, *Deceiving the Sky: Inside Communist China's Drive for Global Supremacy* (New York: Encounter Books, 2019), 167.
[35] Robert Spalding, with Seth Kaufman, *Stealth War: How China Took Over While America's Elite Slept* (New York: Portfolio/Penguin, 2019), 114.
[36] Helberg, *Wires of War*, 155.
[37] Spalding, *Stealth War*, 114.
[38] Manoj Harjani and Gatra Priyandita, "What's Next for 5G in Southeast Asia?," *The Strategist*, October 30, 2023, https://www.aspistrategist.org.au/whats-next-for-5g-in-southeast-asia/.
[39] Ibid.
[40] Helberg, *Wires of War*, 157.
[41] Ibid.
[42] Christopher Woody, "NATO's Top Officer Says We're Living with 'a More Blurred Line between Peace and War'—Thanks to New Russian Tactics," *Business Insider*, September 19, 2018, https://www.businessinsider.com/nato-jens-stoltentberg-world-faces-blurred-line-between-peace-and-war-2018-9.
[43] Agathe Demarais, "What Does 'De-Risking' Actually Mean?," *Foreign Policy*, August 23, 2023, https://foreignpolicy.com/2023/08/23/derisking-us-china-biden-decoupling-technology-supply-chains-semiconductors-chips-ira-trade/.
[44] Ibid.
[45] Helberg, *Wires of War*, 239–240.
[46] Arjun Kharpal, "Netherlands, Home to a Critical Chip Firm, Follows U.S. with Export Curbs on Semiconductor Tools," *CNBC*, June 30, 2023, https://www.cnbc.com/2023/06/30/netherlands-follows-us-with-semiconductor-export-restrictions-.html.
[47] Ibid.
[48] Diksha Madhok, "World's Largest Chipmaker TSMC to Build a Second Factory in Japan," *CNN*, February 7, 2024, https://edition.cnn.com/2024/02/07/tech/tsmc-taiwan-japan-second-factory-intl-hnk/index.html.
[49] Makena Kelly, "Biden Signs $280 Billion CHIPS and Science Act," *The Verge*, August 9, 2022, https://www.theverge.com/2022/8/9/23298147/biden-chips-act-semiconductors-subsidies-ohio-arizona-plant-china.
[50] Gregory C. Allen and Emily Benson, "Clues to the U.S.-Dutch-Japanese Semiconductor Export Controls Deal Are Hiding in Plain Sight," *Center for Strategic and International Studies*, March 1, 2023, https://www.csis.org/analysis/clues-us-dutch-japanese-semiconductor-export-controls-deal-are-hiding-plain-sight.
[51] Annabelle Liang and Nick Marsh, "Gallium and Germanium: What China's New Move in Microchip War Means for the World," *BBC News*, July 31, 2023, https://bbc.com/news/business-66118831.
[52] Ibid.
[53] Lara Seligman, "China Dominates the Rare Earths Market. This U.S. Mine Is Trying to Change That," *Politico*, December 14, 2022, https://www.politico.com/news/magazine/2022/12/14/rare-earth-mines-00071102.
[54] Ibid.
[55] Helberg, *Wires of War*, 98.
[56] Derrick A. Paulo, Tang Hui Huan, Allister D'Souza, and Chubby Jayaram Singh, "China Is King of These Critical Metals. The Battle over Their Supply Has Ensnared Southeast Asia," *CNA*, November 19, 2023, https://www.channelnewsasia.com/cna-insider/china-critical-metals-rare-earths-southeast-asia-ev-battery-3928246.
[57] "Chinese Ships Cut Internet of Taiwan's Outlying Islands," *CNA*, March 8, 2023, https://www.channelnewsasia.com/asia/taiwan-china-ships-cut-internet-outlying-islands-3333376.

[58] David Fickling, "Russia Can Turn Food into a Weapon in Future Crises," *The Print*, March 1, 2022, https://theprint.in/opinion/russia-can-turn-food-into-a-weapon-in-future-crises/852952/.
[59] Matt Burgess, "China Is Relentlessly Hacking Its Neighbors," *Wired*, February 28, 2023, https://www.wired.com/story/china-hack-emails-asean-southeast-asia/.
[60] "Philippines Turns to Hackers for Help as US Warns of China Cyberthreat," *Straits Times*, January 8, 2024, https://www.straitstimes.com/asia/se-asia/philippines-turns-to-hackers-for-help-as-us-warns-of-china-cyber-threat.
[61] Ibid.
[62] Ibid.
[63] Jankowicz, *How to Lose the Information War*, 198.
[64] "China Opposes New Zealand's Accusations of Foreign Interference," *CNA*, August 11, 2023, https://www.channelnewsasia.com/world/china-opposes-new-zealand-accusations-foreign-interference-3693411.
[65] Samuel Chan, "Developing Singapore's Next-Generation Military," *East Asia Forum*, January 2, 2021, https://eastasiaforum.org/2021/01/02/developing-singapores-next-generation-military/.
[66] "POFMA Office," March 27, 2022, https://www.pofmaoffice.gov.sg/.
[67] Ibid.
[68] Jean Iau, "Line Crossed under Foreign Interference Law When People Promote Foreign Political Interests: Experts," *Straits Times*, February 4, 2024, https://www.straitstimes.com/singapore/line-crossed-under-foreign-interference-law-when-people-promote-foreign-political-interests-experts.
[69] Ibid.
[70] "Building a Multicultural Singapore," *SG101*, n.d. https://www.sg101.gov.sg/social-national-identity/multicultural/. This is an official Singapore government agency website.
[71] Mathew Mathews and Hazim Zulfadhli, "In Discussing Israel-Hamas Conflict in Singapore, Upholding Social Harmony Is Key," *Today*, March 6, 2024, https://www.todayonline.com/commentary/commentary-discussing-israel-hamas-conflict-singapore-upholding-social-harmony-key-2376716.
[72] Ajit Mann, "How We Must Battle Weaponized Narrative Wielded by Our Enemies," *Homeland Security Today*, November 23, 2020, https://www.hstoday.us/subject-matter-areas/counterterrorism/how-we-must-battle-weaponized-narrative-wielded-by-our-adversaries/.
[73] Peter Mattis, "China's 'Three Warfares' in Perspective," *War on the Rocks*, January 30, 2018, https://warontherocks.com/2018/01/chinas-three-warfares-perspective/.
[74] P. K. Mallick, "Sneaky Wars," *Indian Strategic Knowledge Online*, May 22, 2023, https://indianstrategicknowledgeonline.com/web/Final%20Mcfarlet.pdf.
[75] Amol Dethe, "You May Not Be Interested in War, but War Is Interested in You," *BFSI*, February 26, 2022, https://bfsi.economictimes.indiatimes.com/news/you-may-not-be-interested-in-war-but-war-is-interested-in-you/89840730.