New England Journal of Public Policy

Volume 34 | Issue 2 Article 5

10-19-2022

Enter the Age of Csywar: Some Reflections on an Emergent Trend

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

Follow this and additional works at: https://scholarworks.umb.edu/nejpp

 Part of the Defense and Security Studies Commons, Infrastructure Commons, Peace and Conflict Studies Commons, and the Science and Technology Policy Commons

Recommended Citation

Ramakrishna, Kumar (2022) "Enter the Age of Csywar: Some Reflections on an Emergent Trend," *New England Journal of Public Policy*: Vol. 34: Iss. 2, Article 5.
Available at: https://scholarworks.umb.edu/nejpp/vol34/iss2/5

This Article is brought to you for free and open access by ScholarWorks at UMass Boston. It has been accepted for inclusion in New England Journal of Public Policy by an authorized editor of ScholarWorks at UMass Boston. For more information, please contact library.uasc@umb.edu.

Enter the Age of Csywar: Some Reflections on an Emergent Trend

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

Abstract

This article uses the current Russian-Ukrainian conflict as a jumping-off point for a broader, preliminary reflection on the continuing evolution of war in the digital age. It is the contention here that we are witnessing an emergent phenomenon of what we might call *csywar*. Intervening states engaged in csywar—best understood as an indirect, hybrid strategy—seek to attain data, infrastructural, and epistemic dominance over the target state. This article discusses various defensive counter-csywar strategies that target states could pursue, such as fostering data, infrastructural, and epistemic resilience internally, and makes the case for developing deterrent counter-csywar capabilities against hostile intervening states.

Kumar Ramakrishna is Professor of National Security Studies, Provost's Chair in National Security Studies, Associate Dean for Policy Studies, and Head of the International Centre for Political Violence and Terrorism Research at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore.

On February 24, 2022, Russia embarked on a "special military operation," seeking the "demilitarization and denazification" of neighboring Ukraine. Russian president Vladimir Putin claimed that he wanted to "to protect people who have been subjected to bullying and genocide . . . for the last eight years." The Ukrainian government quickly dismissed Putin's justification as a pretext.[1] Thoughtful observers agree that Putin's real aim is to re-establish a secure sphere of influence and a Greater Russian "civilizational space" that last existed during the Cold War, covering a region including not merely Russia but "also the Balkans, Ukraine—the historical point of origin for Russian civilization"—and "anywhere Orthodox Christianity is practised or Russian is spoken."[2] In this respect, the Ukrainian government's obvious attempts to seek a closer geopolitical, military, and economic alignment with the West, against the wider context of creeping NATO expansion eastward since the end of the Soviet empire in 1991, was likely adjudged by Putin to be simply unacceptable.[3]

To be sure, the international community has been responding to the Russian invasion of Ukraine with great energy and resolve. So far diplomatic attempts involving multiple governments and international bodies to resolve the conflict between Kyiv and Moscow; indirect military support provided principally through supply of weaponry to the Ukrainian armed forces; heavy and punitive economic sanctions on Russian governmental, business, and commercial entities; and a concerted online information effort to debunk Russian justifications for the invasion have all been employed to isolate the Kremlin, compel it to cease its attacks, and restore the status quo ante.[4]

This article does not seek to add to the already voluminous and rapidly growing analyses of the conflict in Ukraine. Rather, it uses the conflict as a jumping-off point for a broader, preliminary reflection on the continuing evolution of war in the digital age. It is the contention here that at a grand strategic level of analysis, we are witnessing an emergent phenomenon of what we might call *csywar*.[5] Carl von Clausewitz's classic nineteenth-century statement still holds: "War is politics by other means."[6] That is, war is an instrument an intervening state uses to impose its political will on a target state, to change the latter's behavior in ways that advance the interests of the former. Traditionally, kinetic war has been a means of last resort. As evidenced in the Western response to the Russian invasion of Ukraine, the instruments of state power have represented a spectrum of influence involving diplomacy, military force, strategic information operations, and economic policy, including sanctions. In the US context, this idea of a spectrum of power has for many years been encapsulated relatively parsimoniously in the acronym DIME, diplomatic, informational, military, and economic.[7]

As the US military's 2018 *Joint Doctrine Note* explains, the "essence" of the diplomatic instrument is "engagement—how a nation interacts with state or non-state actors, generally to secure some form of agreement that allows the conflicting parties to coexist peacefully." The informational instrument is about "creating, exploiting, and disrupting knowledge" with a view to enjoying "an information advantage over another party." The military instrument can entail "applying force, threatening the application of force, or enabling other parties to apply force in furtherance of strategic ends." Finally, the economic instrument "focuses on furthering or constraining others' prosperity."[8]

While the DIME concept appears to suggest that all four instruments—diplomatic, informational, military, and economic—are of equal importance in national strategy, military theorists have qualified such musings. The eminent military officer and strategic theorist André Beaufre (1902–1975), for instance, distinguishes between direct and indirect strategy. Beaufre classifies these two modes of what he calls "total strategy" "according to the role played by force, ranging from the most insidious to the most violent methods." In "the direct mode military strategy plays a preponderant role; in the indirect mode military force plays a secondary role." Total strategy, according to Beaufre, is "at the top of the strategy

pyramid and is under the direct control of the government," which "decides how all other strategies are coordinated and employed."[9]

Following Beaufre, the state will have to assess the strategic threat posed by an adversary and decide the optimal mix of the four elements of DIME within a total strategic response: if a direct application of DIME were decided upon, then the military instrument would be preponderant, with the other instruments in support. Conversely, if an indirect application of DIME was the approach selected then, the nonkinetic instruments—diplomatic, economic, and informational—would be preponderant in the total strategic response, with the military instrument playing a calibrated supporting role. Beaufre observed that in the Cold War (1945–1990) environment of "nuclear or political deterrence," the "*indirect strategy* . . . [was] very important and not the *direct strategy*'s adoption of material force."[10] Putin's actions in his Ukrainian adventure in February 2022 seems to be a departure from his normal indirect-strategy playbook, in which the military instrument is limited and closely coordinated with diplomatic and informational elements, as in his annexation of Crimea in 2014.[11] In the current undertaking, he appears to be banking on a direct strategy, in which brute military force is the decisive instrument to enable him to attain his geopolitical objectives in Ukraine.[12]

Importance of Indirect Strategy

Since the 1990s, we have witnessed rapid advances in computing power and communication technology, resulting in the rise of the Internet, cheap broadband access, and inexpensive smartphones. With the explosion of social media platforms since the mid-2000s, we are in a position to tweak Beaufre's total strategy ideas, averring that in the contemporary era, indirect strategy is on the ascendant. Employing an indirect strategy, an idea with roots in classical sources much older than Beaufre's treatises, such as the work of the fifth-century BCE Chinese strategist Sun Tzu, essentially involves avoiding the enemy's strength and attacking his weakness instead.[13] The best strategy, according to Sun Tzu, is to "win without fighting."[14] In other words, the ability of one's adversaries to impose their will on us without relying excessively on military power represents the "acme of skill."[15] This basic concept of avoiding strength and attacking weakness sums up efforts by some contemporary observers to explain how, over the past decade, the nonkinetic elements of the DIME model deployed by adversaries have played major roles in undermining the West. For instance, John Carlin argues that the expansion of Internet connectivity "makes our critical infrastructure—water, electricity, communications, banking—and our most private information more vulnerable."[16] He asserts that rather than a cold war, we are now in a "code war," in which "evolving adversaries," ranging from "nation-states, terrorists, criminals, [and] hacktivists" to "single individuals seeking fun, profit, or destruction" could mount devastating cyberattacks that—bypassing the massed strength of a state's conventional armed forces—could directly strike its vulnerable, digitally interconnected homeland and cripple it.[17]

In a related vein, Jacob Helberg argues that we are engaged in a "gray war," in which states like Russia, Iran, and especially China are sidestepping Western military might, seeking digital technologies to "access, delete, and manipulate data" crucial to Western states by gaining greater control of the backend architecture of the global Internet.[18] Calling data the "new oil" and information the "most contested geopolitical resource" sought after by many states, Helberg argues 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."[19] In short, with control of the core layer of the Internet, "you control everything" and can impose your will on the West without resort to costly armed conflict.[20] Peter Singer and Emerson T. Brooking make a broadly similar argument in their book *LikeWar*. Focusing

on the weaponization of social media, they point out that intervening states, by learning how "to command and manipulate" opinion in target states, could foster "political and social polarization" within the latter, rendering them strategically impotent—again without a shot being fired.[21] A former senior military officer and national security adviser to former US president Donald Trump, H. R. McMaster in this respect has argued that Russia under Putin has engaged in "new-generation warfare" with a view to "disrupt, divide and weaken societies" he regards as "competitors."[22]

Russian new-generation warfare—also known as the Gerasimov doctrine after the Russian general who is associated with these ideas[23]—as well as a Chinese version called "three warfares," that is, "psychological warfare, public opinion warfare and legal warfare ('lawfare')"[24]—are also referred to as hybrid warfare.[25] There are several definitions of the concept. A 2010 US Army training document describes it as "the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects."[26] According to an article in the *NATO Review*: "Hybrid warfare entails an interplay or fusion of conventional as well as unconventional instruments of power and tools of subversion. These instruments or tools are blended in a synchronised manner to exploit the vulnerabilities of an antagonist and achieve synergistic effects."[27] In a similar vein, the European Union and NATO define hybrid warfare as "the methods and tools used by individual state or non-state actors to enhance their own interests, strategies and goals," spanning the continuum from "disinformation to disruption of energy supplies, cyber war, and traditional warfare."[28] A key feature of the indirect strategy of hybrid warfare is that it "has blurred the line between peace and war."[29] Analysts have argued that the "internet has delivered nations—and non-nation groups—the ability to engage in actions that appear to step well past the line of peace but fall short of actual war."[30] As the US strategic analyst Sean McFate argues, in the current era there "is no such thing as war or peace—both co-exist, always."[31]

Against the foregoing backdrop, the concept of csywar offers one more preliminary perspective to the growing discourse on the evolving nature of war. It is suggested here that an intervening state engaged in csywar is applying indirect strategy in a hybrid multidimensional fashion. More precisely, in csywar, as we shall see, the intervening state engages in and often integrates assaults on data, infrastructural, and epistemic domains within the target state with one strategic aim: to enable the intervening state to impose its will on the target state. The distinctive feature of the indirect strategy of csywar is that in targeting two of the three target-state domains (data and epistemic), it emphasizes the informational instrument of the standard DIME model. In addition, as we shall see, intervening-state domination of a target state's infrastructural domain can have broader information implications as well. Thus, csywar can be regarded as an indirect strategy of hybrid warfare that prioritizes the application of informational elements of power in the attempt to dominate a target state. That objective is achieved by capturing command of what we may call csywarspace.

Command of Csywarspace: Data, Infrastructural, and Epistemic Dominance

In previous military-technological eras, strategic theorists offered varying assessments of what were the strategic requirements for success in war. While in the nineteenth century Alfred Mahan talked about command of the sea, twentieth-century airpower theorists such as Giulio Douhet promoted command of the air, while the geographer Halford Mackinder proclaimed that whoever commanded the Eurasian "heartland" would control the world.[32] In the emerging csywar era, however, it is suggested that the strategic aim is to secure command of csywarspace. Command of csywarspace is expressed through data, infrastructural, and

epistemic dominance. Data dominance is attained when the intervening state secures relatively unfettered access to confidential public- and private-sector data repositories within the target state, including proprietary information with strategic economic value as well as military-technical secrets. The mining of hacked target-state proprietary data could enable the intervening-state private sector and industrial base to rapidly advance up the technological value chain—without needing to invest the high levels of resources that drove technical innovation by target-state private industry in the first place. This intervening-state-abetted economic espionage could shift the technological, military, and geopolitical balance to the detriment of the target state.[33] In 2010, for instance, the Chinese government was accused of stealing the source code—"the secret back-end recipe for how a website works"—for at least thirty-three US firms, including Google, Yahoo, Symantec, Northrop Grumman, and Dow Chemical, through cyber hacking activities.[34] Under China's 2017 National Intelligence Law, the government can legally require its citizens working in target-state government, technological, and industrial sectors to "acquire data, plans, intellectual property—anything, really—from anyone, anywhere" in a "whatever it takes" approach to become a global leader in cutting edge industries.[35]

For infrastructural dominance, it is postulated that there are minimalist and maximalist scenarios. In the minimalist scenario, the intervening state seeks the unbridled ability to dominate and disrupt the normal functioning of critical target-state infrastructure, such as the Internet, energy, water, and air traffic control systems at will, by distributed denial of service (DDoS) attacks. For instance, when Russian forces invaded the Republic of Georgia in 2008, Georgian websites were hit by botnet-mounted DDoS attacks in one of the earliest examples of hybrid warfare.[36] This massive cyberattack not only "brought down key government websites," it deprived the Georgian authorities of the ability to communicate with the outside world.[37] The maximalist understanding of infrastructural dominance is more worrisome: in essence it involves domination of the world's manufacturing base and supply chains. As of 2015, China produced "28 percent of the world's cars, 41 percent of its ships, more than 60 percent of TVs," and amazingly, "90 percent of the world's mobile phones," while producing half of the world's printed circuit boards—integral to practically all electronic devices.[38] One result of this dominance is the "shocking" extent to which the US military is reliant on "Chinese production"; for instance, US missiles depend on Chinese propellant and US night-vision goggles depend on Chinese specialty metals.[39]

In addition, it has been estimated that as of 2019 China owned 90–95 percent of so-called rare-earth metals, such as dyprosium, neodymium, and gadolinium—critical to the production of "everything from smartphones to hard drives to radar and advanced weapons systems."[40] Another highly significant example of the maximalist goal of infrastructural dominance is China's quest to dominate the backend architecture of the Internet: by 2020, Huawei "controlled approximately 30 percent of the global market share in telecommunications equipment," while making "tremendous progress toward its goal to dominate the emerging market in fifth-generation communications networks."[41] 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."[42] But it also means that an intervening-state-linked telecommunications firm that "builds and controls a nation's 5G network" will have little trouble "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."[43] Thus, maximalist infrastructural dominance opens the door to structural data dominance. In addition, and more ominously, the intervening state could potentially "weaponize" the 5G technology "that is managed by that network" by, for instance, directing self-driving cars into crowds or flying drones into the flight path of commercial aircraft.[44]

The third element of command of csywarspace, epistemic dominance, reaffirms the central importance of the strategic informational thrust of csywar. To achieve epistemic dominance over a target state, an intervening state seeks to shape and mold the perceptions and ultimately the master narrative adhered to by the target-state leadership and its public by ensuring that various combinations of manipulated disinformation and false narratives dominate target-state sociopolitical discourse. With such control of mass attention and sentiment, intervening-state actors can sow confusion and discord between the target state and its public or between different segments of the public. For instance, Russian state propaganda organs such as RT and Sputnik have been described as akin to a "firehose of falsehood" that aims to "disrupt, divide, and weaken societies" that Moscow sees as "competitors."[45]

Achieving epistemic dominance would enable the intervening state to secure political outcomes within the target state favorable to it or even to undermine target-state social and political cohesion. The criticality of epistemic dominance is best illustrated by the concept of the OODA loop developed by the US Air Force officer John Boyd: observe, orient, decide, act.[46] Boyd argues that in interstate geopolitical and strategic contestation, those states that can clearly observe the strategic environment, orient themselves rapidly and accurately to that environment, and efficiently and effectively decide on a course of action and execute it expeditiously would be able to gain a strategic advantage over their adversaries. Boyd argues that states and militaries with tighter OODA loops would be able to outmaneuver adversaries with looser, more dilatory OODA cycles.[47]

Boyd's OODA loop is relevant for the current discussion. If an intervening state is able—through intensive disinformation and false narrative campaigns—to prevent target-state communities from accurately observing and orienting to ground reality, then their decision making and ensuing actions are likely to produce outcomes favorable only to the intervening state, such as lopsided election results and even sociopolitical unrest. Hence, it is important for target states to foster what could be termed observational and orientational accuracy. That is, target-state constituencies—despite a deluge of intervening-state-sponsored online and offline disinformation and biased narratives—must be able to retain an accurate observation of and orientation to ground reality. Failure to do so would risk the target-state society's splitting and polarizing into "alternate realities" in which "groups of like-minded people clump together," growing to "resemble fanatical tribes, trapped in echo chambers of their own design."[48]

In this respect, it is likely that Russian efforts to achieve epistemic dominance by destroying the observational and orientational accuracy of the relevant populations and segmenting them into polarized echo chambers played a key role during the 2016 US presidential elections that led to the election of the pro-Putin candidate Donald Trump as well as in the historic Brexit decision in the United Kingdom—which also served Moscow's geopolitical objective of weakening the democratic European Union.[49] A society clinging to robust observational and orientational accuracy—despite intensive adversarial disinformation and polarization efforts—is thus at the core of target-state attempts to foster epistemic resilience.

Countering Csywar: Fostering Data, Infrastructural, and Epistemic Resilience

To combat intervening-state csywar efforts to secure data, infrastructural, and epistemic dominance, target-state public and private sector stakeholders must develop a broader understanding of what amounts to "critical infrastructure" in the csywar age. While countries have fretted about a "cyber Pearl Harbor" for years, most analysts have narrowly framed this potential as a "devastating attack on our nation's critical infrastructure," such as "our power grid, on our water supply, on hospitals, or on our air traffic control computers."[50] But in 2016,

Russia, as John Carlin argues, attacked another sort of critical infrastructure: "America's confidence in America."[51] Moreover, when North Korean elements in late 2014 hacked Sony Pictures' confidential personnel database to deter the studio from releasing a comedy about a plot to kill its leader, what seemed at first to be a large data breach soon became something more insidious: shaken Sony Pictures employees were also threatened that if they did not speak out against their company they and their families would be harmed as well, because the hackers had accessed their home addresses and other personal information.[52] Intervening-state data dominance could thus enable it to sow confusion and fear within the target state as well. The counter-csywar challenge must thus be framed as broadly as possible. One relatively broad yet parsimonious understanding of the counter-csywar challenge is to frame it as an exercise in building data, infrastructural, and epistemic resilience.

Resilience refers to the ability of actors to safeguard themselves and if necessary bounce back rapidly from unexpected systemic shocks.[53] In our terms, data resilience refers to the ability of public- and private-data owners to protect proprietary information from cyber hacks and theft of intellectual property or to quickly respond to such losses optimally with minimal disruption to their overall functions. Data resilience can be built into target-state institutional cultures by encouraging good habits of individual cyber hygiene. As John Carlin observes, even the most damaging cyber hacks of sensitive data have come through "relatively unsophisticated means exploiting obvious vulnerabilities," including "human frailties, laziness and predictable behaviors"—such as "software patches that haven't been installed, weak or default passwords protecting sensitive data, or 'phishing' techniques where a user has clicked a nefarious link in an email and allowed hackers access to an account."[54] Even information on one's LinkedIn and Facebook pages can be weaponized by intervening-state-linked hackers: an employee at an US "midsized tech company" received an email newsletter from what appeared to be his favorite sports team but was actually a state-sponsored phishing attack that enabled the introduction of a "malicious code that opened a path the company's computer system" and gave the hackers "access to corporate plans, emails, technical specs."[55]

Good cyber hygiene habits that can be encouraged through workshops and continuing education programs are the basic building blocks of effective target-state data resilience.[56] At the same time, effective business continuity plans to respond systematically and optimally to sensitive data breaches are important countermeasures as well.[57] For instance, Estonia's current robust cybersecurity strategy involves emphasizing "end-to-end encryption and two-factor authentication," public-private sector partnerships, "high-functioning e-government infrastructure, digital identity, mandatory security baselines, and a central system for identifying and responding to attacks."[58]

Minimally, infrastructural resilience refers to the ability of public and private entities to protect critical infrastructure networks, such as national power, water supply, and transportation grids, from attempts by malign intervening states to disrupt them and, failing that, to bounce back quickly from such attacks. In a sense, good cyber hygiene and realistic business continuity planning, as described earlier, works well for not just data but also minimalist infrastructural resilience. Maximally, building longer-term infrastructural resilience, in essence, involves reducing over-reliance on intervening-state production-and-supply chain and telecommunications networks for critical target-state national security requirements. For instance, in 2019, when it became clear that "Chinese communications infrastructure combined with a sustained cyber-espionage campaign" threatened target-state national security, the United States, Australia, New Zealand, Japan, and Taiwan "banned Huawei from their networks and urged others to follow suit."[59] At the same time, because of the importance of 5G to "every aspect of citizens' personal lives, corporate world, national infrastructure transportation, health, and national defense," some observers argue that multinational collaboration is needed to develop trusted 5G telecommunications that can

"protect sensitive and proprietary data."[60] Jacob Helberg adds that the US Congress should authorize a National Advanced Manufacturing Strategy to reduce US "dependence on Chinese supply chains and revitalize American manufacturing," especially in the areas of "semiconductors" and "high-performing microchips, which are used in "everything from artificial intelligence to cell phones."[61] He calls for more systematic government scrutiny of "which high-tech and vital goods must be produced domestically, which can be safely sourced from an Allied Industrial and Innovation Base, and which goods can still be imported" from more general sources.[62]

Finally, epistemic resilience in the current analysis refers to the ability of target-state stakeholders to cope effectively with intervening-state-supported online and offline disinformation campaigns, in the process ensuring that the body politic retains access to objective information and relatively unbiased narratives that are largely reflective of reality—thus preserving their collective observational and orientational accuracy.

Observational accuracy can be enhanced by rapidly calling out online disinformation when it appears. In Singapore, for instance, the Protection from Online Falsehoods and Manipulations Act (POFMA), passed in June 2019, "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." 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."[63] Germany, France, and Thailand have also introduced legislation that grants "authorities more executive power to deter fake news, allowing them to force social media platforms, websites, and publishers to remove false content."[64] As Nina Jankowicz points out, however, "decades of political science and psychological research" suggest that laws that mandate "fact checks" may "not only fail to correct falsehoods, they often cause individuals to double down on incorrect information."[65] In addition, disinformation disseminated through encrypted messaging apps that cannot be openly tracked cannot be debunked: "Fact-checking can't help us dispel claims made in private fora."[66]

The preceding analysis compels some analysts to argue with Singer and Brooking that the key really is "*information literacy*," which should be inculcated from childhood on and is "*no longer merely an education issue but a national security imperative*."[67] The University of Washington, for instance, runs courses on "advanced critical thinking in media consumption," such as the colorfully titled "Calling Bullshit: Data Reasoning in a Digital World."[68] In Ukraine, an American NGO called IREX has collaborated with the Academy of Ukrainian Press and the fact-checking entity StopFake to run an information literacy-promoting curriculum called "Learn to Discern." The curriculum is described as more practical than academic and trains media consumers to "recognize emotional manipulation"—a technique used by "purveyors of disinformation from Russia and beyond"—so that they can "read news more critically."[69]

The "Learn to Discern" program has produced results: trained consumers have engaged in "cross-checking multiple news sources" and have shown "sophisticated knowledge of the news industry."[70] Similarly, Finland—long targeted by propaganda from neighboring Russia—emphasizes critical thinking skills in the education system beginning in the early grades, to the extent that "Finns rank at the top of all Europeans in their ability to resist fake news."[71] At the same time, in an effort to thwart the formation of online echo chambers, a US start-up called Soap AI has designed a "machine learning platform that allows users to understand better what is happening in the world by accessing verified sources of information, reducing the clutter associated with clickbait, and ensuring access to a range of perspectives." In short, the Soap

platform "presents multiple opinions on an event or story so readers can make their own judgments based on correct information."[72]

Attaining epistemic resilience in the target-state body politic also depends, as John Boyd suggests, on orientational accuracy. That is, what attitudes and worldview would the community adopt toward incoming news and information after the observation phase? The answer to this question is important because orientation, as noted, would impact the decision and action phases. In his OODA loop model, Boyd points out that orientation is affected not just by incoming information but also by "previous experience," "cultural traditions," and prevailing "analyses and synthesis."[73] For this reason, observational accuracy is not enough: even if disinformation and false narratives have been largely filtered out in the observational phase, orientational accuracy can still be impacted by extant sociopolitical fault-lines that can be weaponized by intervening-state organs. As Jankowicz points out, from the Russian perspective, in Estonia such weaknesses included "ethnic tensions and historical revisionism"; in Georgia, "culture and religion"; in Poland, "political polarization"; and in the Czech Republic, "anti-migrant sentiment."[74] She observes—wisely—that "unless we mitigate our own political polarization, our own internal issues, we will continue to be an easy target for any malign actor" to attack—with consequences for target-state political and social cohesion.[75]

Responding to Csywar: Are We Ready?

The emergent indirect hybrid strategy of csywar, in which an adversarial intervening state seeks to bypass a target state's strengths and hammer away at its internal weaknesses by attaining data, infrastructural, and epistemic dominance may well reflect an inflection point in the continuing evolution of warfare. There have been similar inflection points in the past. While strategic theorists such as Clausewitz and Antoine Henri Jomini earned acclaim for explaining the new European age of Napoleonic destructive mass warfare in the early nineteenth century,[76] a century later, nuclear strategists such as Bernard Brodie arrived at the paradoxical analysis that the overriding value of atomic weapons was to flaunt them but never use them.[77] A new generation of strategic analysts is now trying to come to grips with what has been called "likewar," "gray war," and "code war." In this article I have suggested another hopefully useful term to add to the growing literature on hybrid warfare: csywar.

The current Russian invasion in Ukraine may well signify the beginning of a wider geopolitical conflict between a US-led Western liberal democratic bloc and an authoritarian axis involving Russia and China and its allies—a new cold war based on csywar principles. After all, in 2019 Putin declared that "liberalism" had "become obsolete,"[78] while he and Chinese president Xi Jinping proclaimed in early February 2022 that their strategic partnership had "no limits"—though the veracity of that assertion is currently being tested in the current conflict in Ukraine.[79]

While countering intervening-state csywar campaigns by fostering data, infrastructural, and epistemic resilience is important, these measures are strategically defensive. It may well be important for the international community of democratic states also to consider deterrent counter-csywar measures. Just as mutual nuclear deterrence kept the Cold War from getting hot, national target-state capabilities to deter aggressive intervening states are needed to help preserve the integrity of target-state csywarspace. In this regard, democratic target-state policy and strategic elites must ask whether they possess realistic response options short of military force, ranging from legal and diplomatic challenges and economic sanctions to credible cyber and informational offensive capabilities—singly or in coordination with allies—that potentially aggressive intervening states must take into account and may well encourage the latter to commit to more reasonable overall behavior.[80]

Three points can be made in this regard. First, target states seeking to deter and if necessary respond more assertively to csywar attacks should be clear about what the threshold for an attack in csywarspace triggering counter-csywar measures looks like. As Helberg puts it, in the Cold War, "threats came by way of intercontinental missiles," but today "the new ICBM is an IBM."[81] Target states should thus develop a counter-csywar doctrine that specifies a range of responses to intervening states "proportionate to the scale and effect of the initial assault."[82]

Second, an offensive plank of a target state's counter-csywar strategy should also include active deterrence of intervening states by the credible threat of highly effective target-state-mounted epistemic dominance campaigns capable of undermining the domestic and geopolitical standing of rogue intervening-state regimes. For instance, because of the current travails of the Russian invasion force in Ukraine, the international, economic, and domestic political fallout of Western sanctions—on top of Putin's very real domestic weaknesses—there is seems to be ample scope for target-state strategic communities to beat the Russians at their own game, though in this instance, "truth and transparency" would be "important offensive as well as defensive weapons to defeat the Kremlin's use of lies and obfuscation."[83]

Finally, depending on how the post–Ukraine conflict geopolitical landscape pans out, an effective coordinated democratic state total strategy for international stability may require the creation of a democratic "techno-bloc of nations" based on "Internet infrastructure free of authoritarian influence," to strike a new global balance of power with an emergent authoritarian techno-bloc led by China and Russia.[84] In sum, the burning question is clear: Are we ready to respond to the emergent Age of Csywar?

Notes

[1] "Putin Orders 'Special Military Operation' to 'Denazify' Ukraine," *Haaretz*, February 24, 2022, https://www.haaretz.com/world-news/europe/putin-authorizes-special-military-operation-to-denazify-ukraine-1.10631507.

[2] David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (London: Hurst and Company, 2020), 135.

[3] Ted Galen Carpenter, "Many Predicted NATO Expansion Would Lead to War. Those Warnings Were Ignored," *Guardian*, February 28, 2022, https://www.theguardian.com/commentisfree/2022/feb/28/nato-expansion-war-russia-ukraine.

[4] Jamie Shea, "Russia's Invasion of Ukraine: Getting the Right Strategy in Place," *Friends of Europe*, March 4, 2022, https://www.friendsofeurope.org/insights/russias-invasion-of-ukraine-getting-the-right-western-strategy-in-place/.

[5] This article expands on the shorter analysis in Kumar Ramakrishna, "The Advent of 'Cywar': Are We Ready?," *RSIS Commentary*, January 21, 2019, https://dr.ntu.edu.sg/bitstream/10220/47562/1/The%20Advent%20of%20%E2%80%9CCyWar%E2%80%9D%20Are%20We%20Ready.pdf. I have slightly amended the term to "csywar" to better capture the cyber-infrastructural and psychological (psywar) elements that are blended within the concept.

[6] Peter Paret and Michael Howard, eds., *Carl von Clausewitz, On War* (Princeton: Princeton University Press, 1976).

[7] *Joint Doctrine Note: Strategy* (Washington D.C: Joint Force Development Branch, April 25, 2018), vii–viii; II-5-II-7. The document asserts that while the DIME model is widely used to describe the "instruments of national power," there are "many more instruments involved in national security policy development and implementation."

[8] Ibid., II-5-II-7.

[9] 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/.

[10] Ibid.

[11] Marcel H. Van Herpen, *Putin's Wars: The Rise of Russia's New Imperialism,* 2nd ed. (Lanham: Rowman & Littlefield, 2015), 271–272.

[12] Stephanie Sy and Dan Sagalyn, "Why Russia is Increasingly Using Brutal Tactics in Ukraine," *PBS Newshour*, March 10, 2022, https://www.pbs.org/newshour/show/why-russia-is-using-increasingly-brutal-tactics-in-ukraine.
[13] Mark R. McNeilly, *Sun Tzu and the Art of Modern Warfare* (New York: Oxford University Press, 2015).
[14] James Holmes, "Win without Fighting? Sun Tzu, and History, Says You Can," *The National Interest*, June 8, 2021, https://nationalinterest.org/blog/reboot/win-without-fighting-sun-tzu-and-history-says-you-can-187117.
[15] "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/view/10.1093/acref/9780191843730.001.0001/q-oro-ed5-00010536.
[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., 44–45.
[18] Jacob Helberg, *The Wires of War: Technology and the Global Struggle for Power* (New York: Avid Reader Press, 2021), 155.
[19] Ibid., 134–135, 157.
[20] Ibid, 145.
[21] P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt, 2018), 126–127.
[22] H. R. McMaster, *Battlegrounds: The Fight to Defend the Free World* (New York: Harper, 2020), 40–41.
[23] Ibid., 40.
[24] Kilcullen, *Dragons and the Snakes*, 211.
[25] Other oft-used terms include "gray zone operations," "asymmetric warfare,, and "non-linear warfare." See ibid., 150.
[26] Nina Jankowicz, *How to Lose the Information War: Russia, Fake News, and the Future of Conflict* (London: I. B. Tauris, 2020), 162.
[27] Arsalan Bilal, "Hybrid Warfare: New Threats, Complexity and 'Trust' as the Antidote," *NATO Review*, November 30, 2021, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html#:~:text=To%20put%20it%20simply%2C%20hybrid,antagonist%20and%20achieve%20synergistic%20effects.
[28] Jankowicz, *How to Lose the Information War*, 162.
[29] Carlin, *Dawn of the Code War*, 57.
[30] Ibid., 58.
[31] Sean McFate, *The New Rules of War: Victory in the Age of Durable Disorder* (New York: HarperCollins, 2019), 59.
[32] Theodore Ropp, "Continental Doctrines of Sea Power," in *Makers of Modern Strategy*, ed. Edward Mead Earle (Princeton, NJ: Princeton University Press, 1944); Claudio G. Segre, "Giulio Douhet: Strategist, Theorist, Prophet?," *Journal of Strategic Studies* 15, no. 3 (September 1992): 351–366; Hans W. Weigert, "Mackinder's Heartland," *American Scholar* 15, no. 1 (Winter 1945–1946): 43–54.
[33] Carlin, *Dawn of the Code War*, 146–147.
[34] Ibid., 181.
[35] Robert Spalding, with Seth Kaufman, *Stealth War: How China Took Over While America's Elite Slept* (New York: Portfolio/Penguin, 2019), 146–147.
[36] Carlin, *Dawn of the Code War*, 158.
[37] Jankovic, *How to Lose the Information War*, 60–61.
[38] Helberg, *Wires of War*, 97.
[39] Ibid., 98.
[40] Spalding, *Stealth War*, 78.
[41] McMaster, *Battlegrounds*, 141.
[42] Bill Geertz, *Deceiving the Sky: Inside Communist China's Drive for Global Supremacy* (New York: Encounter Books, 2019), 167.
[43] Spalding, *Stealth War*, 114.
[44] Ibid.
[45] McMaster, *Battlegrounds*, 41.
[46] Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (New York: Back Bay Books, 2002), 334–335.
[47] Byrne Hobart, "Investing Inside the OODA Loop," Medium.com, May 30, 2019, https://medium.com/swlh/investing-inside-the-ooda-loop-17356c4a6ceb.
[48] Singer and Brooking, *LikeWar*, 123, 137.

[49] Nafeez Ahmed, "Trump Military Study Saw 'Brexit' as 'First Step' of Russian 'Information Blitzkrieg' on West," *Byline Times*, March 2, 2022, https://bylinetimes.com/2022/03/02/trump-military-study-saw-brexit-as-first-step-in-russian-information-blitzkrieg-on-west/.
[50] Carlin, *Dawn of the Code War*, 61.
[51] Ibid.
[52] Ibid., 308–339.
[53] The literature on resilience in extensive. For instance: Stephen E. Flynn, "America the Resilient: Defying Terrorism and Mitigating Natural Disasters, *Foreign Affairs* (March/April 2008), https://www.foreignaffairs.com/articles/2008-03-02/america-resilient; David Denyer, *Organizational Resilience: A Summary of Academic Evidence, Business Insights and New Thinking* (Cranfield: BSI and Cranfield School of Management, 2017).
[54] Carlin, *Dawn of the Code War*, 50.
[55] Spalding, *Stealth War*, 98–99.
[56] Helberg, *Wires of War*, 230.
[57] See for instance, "Business Continuing Planning," *EC-Council*, 2022, https://www.eccouncil.org/business-continuity-planning/#:~:text=Business%20Continuity%20Planning%20(BCP)%20is,during%20execution%20of%20disaster%20recovery.
[58] McMaster, *Battlegrounds*, 75.
[59] Ibid., 139.
[60] Ibid., 142–143.
[61] Helberg, *Wires of War*, 239–240.
[62] Ibid., 240.
[63] "POFMA Office," March 27, 2022, https://www.pofmaoffice.gov.sg/.
[64] Ryan Chua, "Looking beyond POFMA to Combat Fake News and Misinformation in Singapore," *Singapore Policy Journal*, October 24, 2021, https://spj.hkspublications.org/2021/10/24/looking-beyond-pofma-to-combat-fake-news-and-misinformation-in-singapore/#_edn7.
[65] Jankowicz, *How to Lose the Information War*, 202.
[66] Ibid.
[67] Singer and Brooking, *LikeWar*, 264.
[68] Ibid.
[69] Jankowicz, *How to Lose the Information War*, 216.
[70] Ibid., 217.
[71] Helberg, *Wires of War*, 260–261.
[72] McMaster, *Battlegrounds*, 76–77.
[73] Coram, *Boyd*, 344.
[74] Jankowicz, *How to Lose the Information War*, 198.
[75] Ibid., 198–199.
[76] W. E. Linde, "Clausewitz, Jomini, and the Birth of Modern Strategy," *Fog and Friction*, May 1, 2015, https://fogandfriction.com/2015/05/01/clausewitz-jomini-and-the-birth-of-modern-strategy/.
[77] Bernard and Fawn M. Brodie, *From Crossbow to H-Bomb: The Evolution of the Weapons and Tactics of Warfare*, revised and enlarged edition (Bloomington: Indiana University Press, 1973).
[78] McMaster, *Battlegrounds*, 78.
[79] Anna Kireeva, "The Limits to Russia and China's 'No Limits' Partnership," *East Asia Forum*, March 23, 2022, https://www.eastasiaforum.org/2022/03/23/the-limits-to-russia-and-chinas-no-limits-friendship/.
[80] Ramakrishna, "Advent of Cywar."
[81] Helberg, *Wires of War*, 211.
[82] Ibid., 211–212.
[83] McMaster, *Battlegrounds*, 80–81.
[84] Helberg, *Wires of War*, 210–211.