CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

APRIL 2023 | CYBER CONFLICT IN THE RUSSIA-UKRAINE WAR

Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict

Ariel E. Levite

Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict

Ariel E. Levite

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Introduction

It is too early to draw definitive conclusions about cyber warfare in the lead-up to and the execution of the Ukraine war. Data are lacking, and the outcome of the conflict remains uncertain. Yet through monitoring and analysis of a single year in the first major war into which cyber has been extensively woven, we do know enough to be able to generate some tentative, high-level, generic propositions on the nature of cyber conflict. These propositions draw on wide-ranging press reporting and extrapolate from several superb pieces recently published by my colleagues Jon Bateman, Nick Beecroft, and Gavin Wilde, as well as Microsoft's recent report on the cyber dynamics of the conflict.[1]

However, we must still tread cautiously. Our propositions draw on highly imperfect empirical knowledge of a single historical case that is still unfolding.[2] Current and future antagonists are also constantly learning from their own and others' analyses and enhancing their performance, which can render current assessments obsolete.[3] For this and other reasons it is quite possible that some of the cyber dynamics unfolding in and around Ukraine may play out differently later in Ukraine as well as in other, future confrontations. As we have observed over millennia, the balance between offense and defense can shift over time; this dynamic may well play out in cyberspace as well.

It is also important to note at the outset that widespread assessments disparaging the utility and expediency of Russian cyber operations in the Ukrainian conflict (and projections regarding future conflicts) are presently limited by far more than a lack of comprehensive and reliable empirical data. We also lack insights into the metrics and criteria that each of the protagonists uses to assess the success and failure of cyber's overall performance in

the conflict, and we have only fragmentary evidence of the role each party expected cyber operations to perform. Moreover, even if we had such information, Ukraine-specific answers might not apply elsewhere because the expectations for cyber and the metrics for assessing its performance may vary not only over time and between protagonists but also from one conflict to another. In this context it is important to underscore that some specific factors that possibly helped diminish the efficacy of Russia's offensive cyber operations in Ukraine may not apply elsewhere. Three in particular deserve to be noted here: Russia's unique approach toward cyber warfare; the level of external support that Ukraine received before and during the war from some leading national and multinational cyber powers; and the sophistication and battle-tested experience of Ukraine's cyber warriors.[4]

Nevertheless, even if some of the cyber characteristics of the Ukraine conflict ultimately turn out to be sui generis, they are instructive given the novelty of the field and the involvement of major powers in the conflict. Hence, there is considerable value in advancing these propositions to focus attention on certain questions and facets of cyber conflict, facilitating their review and reassessment as more comprehensive and reliable information becomes available and developments on the battlefield evolve. But the reader should consider the interim observations and propositions offered here as hypotheses employed as a heuristic to encourage debate and invite feedback.

All the propositions offered below pertain to our core conception of what cyber warfare is about. Some of the propositions we advance are novel; others reaffirm or refine tentative assertions made before the war. Taken together they suggest a more subdued view of the utility and impact of cyber warfare than was generally found in prewar speculations. More importantly, the Ukraine war reveals that nations diverge significantly in the role and aims they assign to offensive cyber operations as well as the institutional setup and operational modalities they use for conducting them. Most glaringly, the U.S. perspective and approach (emulated in whole or in part by several other Western nations) differs deeply from that of Russia, which makes it reasonable to expect similar divergence across similar regimes.

We group our propositions under three temporal headings: the prewar period (starting in 2014);[5] the war itself (beginning on February 24, 2022); and finally, the postwar period, after kinetic hostilities eventually die down. Obviously, we cannot know when this last phase will begin; nevertheless, analysis of trends that were manifest in the two earlier phases of the conflict provides a tentative basis for predictions as to what might be expected down the road. This broad scope is driven by two considerations. First, it is designed to underscore the considerable relevance of cyber operations across various phases and types of conflicts. And second, it highlights continuity as well as change between cyber action in peacetime, in wartime, and in grey area situations, as well as during the transitions between these states of confrontation.

The Prewar Period

The Preeminence of Cyber Intelligence

The massive, ubiquitous, and universal transition to digital media and communications and the growing dependence on the services they provide has also dramatically transformed intelligence operations. It has made cyber intelligence into a prominent component not just of intelligence (and counterintelligence) collection efforts but also of covert operations, influence missions, and information warfare. Cyber intelligence is capable of encroaching not only on the confidentiality of data but also on their integrity and availability. It similarly affects the processes, systems, and analysis that depend on that data. What started out as a singularly dominant U.S. capability is now widely valued and distributed not only to nation-states but to other governmental and nongovernmental actors. Thus, it is hardly surprising that in the Ukraine conflict all protagonists have been conducting extensive cyber intelligence operations.[6]

Starting long before the military confrontation, and at times when the escalation toward a full-fledged war was anything but given, Ukraine's growing level of sophistication in the digital domain and dependence on digital assets have made cyber intelligence a constant factor in intelligence confrontation between Russia and Ukraine. Yet Russia appears to still be wedded to prioritizing human intelligence (HUMINT) over any other form of intelligence operations, while Ukraine's own capabilities have been considerably bolstered by massive assistance, starting in 2021, from foreign governments and corporations.

Organic Ties Between Intelligence and Cyber Operations

The Ukrainian case also highlights the organic ties between cyber operations and other intelligence functions, missions, and operations. To some extent this is a generic phenomenon, as both offensive and defensive cyber operations typically initially emerge within intelligence organizations and have many common prerequisites and attributes. Hence, they retain close ties to intelligence, especially when no large-scale military operation is underway. Yet in the West defensive and offensive cyber operations commonly grow gradually into separate institutional entities, subject to independent chains of command as well as legal/policy regimes. What the Ukraine conflict demonstrates, however, is that no such evolution has occurred in Russia; there, cyber operations remain closely linked (and subordinate) to intelligence both organizationally and culturally, certainly in the prewar period and perhaps also during the war itself.

In the Ukraine conflict, the cyber intelligence nexus has manifested in at least two aspects. The first is Russian leaders' emphasis on HUMINT as a key enabler of their entire planning for the Ukraine campaign, including cyber operations.[7] From the time they possessed de facto control of Ukraine, Russian cyber operators seem to have leveraged insider information and threats both to bolster their influence operations and to gain access to Ukrainian IT assets: tapping local agents and collaborators and their intimate knowledge of and access to Ukrainian infrastructure to facilitate cyber operations for intelligence gathering, harassment, subversion, and sabotage.[8] The second remarkable feature has been Russia's institutional (and political) treatment of Ukraine as an extension of the Russian home front in terms of intelligence and cyber operations as well as institutional responsibility for carrying them out.[9]

But Russian cyber operations in Ukraine prior to the war may actually tell a bigger story. Such operations have been to an important degree an extension of domestic Russian cyber intelligence.[10] This may be due to the unique features of the Russian–Ukrainian relationship arising from their remarkable historical intimacy (political, cultural, demographic, and religious) as well as their geographical contiguity. But it may also stem from the fact that in Russia (unlike in most NATO members and many other nations) cyber operations have been organizationally and culturally subordinate to intelligence, both in prewar times and to an important degree even during wartime.

Cyber Attacks Are Not (Yet?) Considered War

Lawyers, diplomats, and experts generally agree that international law applies (in principle) to cyberspace. Yet they have long and inconclusively debated *how* it applies and, most pointedly, when cyber attacks cross the threshold to be legitimately considered acts of war.[11] This is an important debate yet one that is hardly likely to yield a broad consensus. Sharp disagreements between key participants remain, and some leading parties want to leave themselves considerable elbow room to interpret and reinterpret how applicable core legal principles should be operationalized.

Since 2014, the Ukraine conflict has seen sustained and massive cyber intelligence operations and even cyber attacks (what Jon Bateman has termed "cyber fires") conducted mostly by Russian state organs and sometimes apparently by proxies. These have included highly disruptive and even destructive operations against critical Ukrainian infrastructure, such as its energy generation and distribution systems.[12] Yet at the time these were not considered to cross the threshold of war, even by Russia's Western adversaries. In fact, the lines between legitimate and illegitimate peacetime penetrations of adversary cyber networks have been consistently blurred and contested—and not solely by China and Russia, much as these nations' activity seems at times particularly reckless.

The United States and Israel are cases in point. Even in "peacetime," the United States has at least occasionally gone beyond extensive penetration of adversary networks for (passive) intelligence collection purposes; such activity has also been undertaken for the proactive

defense of the United States' and allies' networks (including those in Ukraine). This practice has more recently been formalized under U.S. Cyber Command (USCYBERCOM)'s much-touted doctrine of "defend forward/persistent engagement."

The United States has actually gone further, engaging at times in cyber attacks designed to incapacitate its adversary's activity. Although activities of this nature are typically shrouded in extreme secrecy, they are known to have taken place against the Iranian nuclear program in an operation widely known as Olympic Games, which was intended to cause damage, albeit of a highly localized and precise nature; a similar operation was later used to incapacitate the Islamic State (ISIS). Israeli cyber actions, conducted alone and with the United States, especially against Iranian assets and installations, seem to fall into the same category. Both nations apparently consider their actions perfectly legitimate and legal in nonwar settings and as such materially different from Russian actions in Ukraine. They appear to have judged their own actions to meet the key policy and legal requirements upheld by international law (that is, that acts of aggression be necessary, proportionate, and discriminate), having carefully designed their operations to produce temporary, precise, and localized effects on military-usable assets and facilities.

The key takeaway from this discussion is that some of the most significant cyber powers appear to have concluded that offensive cyber actions in peacetime, even those that go well beyond intelligence collection, do not automatically constitute armed attacks, let alone acts of war. Heretofore, neither the character of the cyber operations, nor the highly adversarial context in which they occur, nor their targets and effects (even when incapacitating such sensitive facilities as critical infrastructure) have proven sufficient to get the international community to accord them the status of an "armed attack," much less an "act of war." Even the protagonists themselves appear to concur, as can be seen from the ever-escalating offensive cyber exchanges between Iran and Israel that were not considered by either party to fall into these categories. In fact, the actions and diplomacy of those employing offensive cyber means as well as those on the receiving end have now created a both a clear and consistent pattern and a series of precedents suggesting that cyber protagonists wish to leave themselves considerable latitude to interpret their adversaries' offensive cyber action on a case-by-case basis. No less importantly, the behavior of these parties reveals that many prefer to retain broad latitude to undertake such actions themselves.

Notwithstanding this commonality, parties are still likely to differ some on where and how they draw the line. Consequently, one cannot exclude the possibility that if cyber were used as a principal means for a strategic attack that caused significant loss of life, it might be deemed an armed attack. NATO, for one, has been recently evolving its approach to reflect such thinking.[13] While such a posture may prove appealing from a policy perspective, it nonetheless sets the bar rather high on the criteria that must be met for offensive cyber action to be seriously considered warlike; it also leaves the determination of whether (and when) these criteria have been met to case-by-case judgment after the fact, thereby detracting some from its normative and deterrence value.

Serious Advance Preparations for Attacks Are Necessary

For offensive cyber operations to have a relatively high likelihood of success,[14] extensive preparatory operations are required well in advance that go quite far along Lockheed Martin's Cyber Kill Chain.[15] Clandestine infrastructure must be created to penetrate adversary networks, establish a secret foothold, reconnoiter the entire network, and establish a command-and-control apparatus. Additional comprehensive preparations are also essential to convert this foothold into a physical attack on valuable digital assets that will either neutralize them or take them over and leverage them to conduct follow-on digital attacks. In either case the preparations must develop full-fledged options for generating the desired impacts, either when certain criteria are met or on demand. In Ukraine this involved Russia repeatedly probing and testing the cyber defenders' capabilities and routines.

Advance cyber attack preparations seem to create a powerful first-strike advantage. The incentive to launch cyber attacks early, before conventional confrontation begins, is predicated on two considerations: to help carry out subsequent conventional operations and to do so before operational developments diminish the likelihood that the planned cyber attacks would accomplish their intended effects (a cyber manifestation of the generic "use it or lose it" syndrome). Indeed, as Jon Bateman has observed, the most prominent Russian cyber attacks were carried out very early in the war. Such attacks largely faded thereafter, suggesting that their operators may indeed have sought to unleash their most sophisticated attacks (such as the targeting of Viasat to incapacitate key telecommunication systems) ahead of the conventional attack. The incentives to strike early/first appear especially powerful for cyber powers like Russia that are less agile in detecting and attacking new targets on the fly. Naturally, though, advance preparations as well as the incentives to attack early/first involve painful political and operational trade-offs.

Substitution, Synergy, and Trade-offs Between Cyber Operations and Conventional Attack Planning

We must also consider the likelihood that Russian cyber operations against Ukraine, prior to the invasion of Crimea in 2014 and up to the February 2022 attack, have probably served much more than immediately observable tactical and operational purposes.[16] The most likely purpose was probably to suppress and dissuade Ukraine's "drift to the West" through operations short of war. Yet in practice (and perhaps later also by design) these operations must have also provided Russia with up-to-date, firsthand familiarity with Ukrainian networks as well as their defenders' capabilities and modus operandi that Russia could leverage once they began to seriously contemplate escalation toward an all-out military campaign.

In addition, the prewar cyber interaction between Russia and Ukraine seems to have had three important downsides. First, Russian prewar cyber operations in and against Ukraine may have had an escalatory impact, further intensifying the rivalry between Russia and Ukraine. Second, they alerted Ukrainians (and just as importantly their friends and allies)

to the cyber challenge Ukraine faced, encouraging authorities to improve their vigilance and capabilities, to cue their defensive preparations, and to forge collaboration with Western allies especially in the period leading up to the 2022 invasion. The net effect may have advantaged Ukraine. Third, although mostly undertaken in extreme secrecy and under deep cover, Russian cyber operations seem to have unintentionally emitted telltale signs that tipped off the Ukrainians (directly and via their allies) about what Russia had in store for them both strategically (that an attack was contemplated) and tactically (the specific targets threatened), thereby facilitating defensive preparations of all sorts, not least in the form of counter–cyber operations.

In the final analysis, then, the Ukraine case seems instructive on some of the trade-offs associated with use and pre-positioning of offensive cyber tools in nonwar situations. Such strategies serve both immediate and long-term functions, yet these benefits come at a cost and risk that are anything but negligible. Parties contemplating offensive cyber use in the future would undoubtedly have to weigh these trade-offs and strike a balance between them prior to applying offensive cyber in other conflicts.

It Is Challenging to Predict and Bound the Cyber "Blast Radius"

The above discussion forces us to consider cyber operators' capacity to predict and bound the effects of their operations. There is an analogy here to military operations research. Since its inception in World War II, this discipline has progressed to the point of being able to generate fairly accurate estimates of the effects of kinetic attacks. Originally driven by desire to maximize the impact on the intended targets, this discipline over time has become an important catalyst for and facilitator of the effort to reduce collateral damage and unintended effects on noncombatants. The interest in reducing unintended effects has in turn served to calibrate expectations and shape norms governing behavior in combat that over time have been codified in doctrines and protocols.

Yet similar progress in cyber lags far behind, partially due to the novelty of the field and partially due to the much greater challenges presented by a highly complex, interdependent, and rapidly evolving digital space. Factors such as offensive cyber operators' temptation to enhance the effects of their actions or reach otherwise inaccessible targets (for example by employing cyber worms that spread laterally and vertically) accentuate an attack's potential to cascade beyond cyberspace and reverberate in the physical and cognitive realms. Such dynamics further complicate efforts to bound effects, whether for legal or operational reasons or both. It is against this background that we need to assess Russian cyber operations against Ukraine between 2014 and the onset of war in 2022.

By all accounts, cyber operations during this period occasionally resulted in significant collateral damage, especially on the Ukrainian side, but in some instances also well beyond it. NotPetya was the most dramatic, publicly known example of such damage spreading to other countries and numerous civilian entities.[17] But whereas Russian conduct in the more

recent phases of the war clearly sought to inflict maximal collateral damage in Ukraine, it remains uncertain for now whether the collateral damage inflicted by Russian cyber operations prior to the kinetic war was intentional. And if it was not, was it because the Russian operators could do no better (lacking the capacity to anticipate such spillover), were indifferent to it, or consciously opted for indiscrimination as a means of enhancing the impact of their cyber operation?

Collateral Damage: An Asset or a Liability?

Much of the peacetime appeal of cyber operations derives from their unique value proposition in shadowy conflicts thanks to their relatively low signature, transient effects, and localized impact. Realizing this potential, however, depends on the (heretofore limited) capacity to predict and bound the blast radius in cyber operations. It takes an exceptional combination of determination, sophistication, and effort to accomplish the intended results from a cyber intrusion and confine its impact to its primary intended target while also denying others the opportunity to replicate, reverse engineer, or leverage tools and vulnerabilities exposed in the course of the operation. This challenge imposes a serious limiting factor on the conduct of such operations in peacetime.

But in the lead-up to the Ukrainian war, Russia consistently failed to uphold this standard. At a minimum Russia has dispensed with the requirement that it be able to limit the blast radius of its cyber intrusions and perhaps has even sought to maximize it. Yet Russia has not yet paid a heavy price for this cyber modus operandi. This sets a rather ominous precedent that may shape future Russian cyber conduct as well as that of others pondering similar actions: namely that they can engage in peacetime offensive cyber operations without risking serious consequences for doing so. The lack of clear international judgment on the legality of Russia's cyber operations and the failure to impose consequences specifically for them could thus lower the bar for the indiscriminate use of cyber power, especially in peacetime. Other states that thus far may have held back from such action may reconsider their calculus, especially if they lack high-end capabilities to undertake cyber operations surgically and clandestinely.

Russian and American Conceptions of Cyber Operations Contrast Sharply

Most nations operate in cyberspace to collect intelligence and assist law enforcement operations. Many also are gearing up to conduct military cyber operations in wartime. The United States and Russia are no exception. Both (as well as some other Western nations) employ cyber means as instruments of counterterrorism (and for the United States counterproliferation) as well as for signaling, particularly for deterrence purposes. In this context it is worth comparing the Russian December 2015 attack against part of the Ukrainian electric grid and Operation Olympic Games, conducted by the United States (with the widely assumed assistance of Israel) against the Iranian centrifuge enrichment program.[18] Both were

elaborate and highly sophisticated attacks. The U.S. operation sought to temporarily disrupt an Iranian path to acquisition of weapons-grade fissile material. The Russian attack, as far as we can tell, was in retaliation for a Ukrainian strike at Russia's energy supply and aimed to put Ukrainians on notice of what Russia could do if Ukraine struck at vital Russian assets again. It employed a (locally) measured and carefully calibrated amount of disruption and destruction. What sets these operations apart is primarily the Russian willingness to cause extensive collateral damage during its operation, contrasted against the United States' exceptional caution to avoid doing so.

This comparison, in fact, attests to an even a bigger divergence in the modalities employed by the two nations in their peacetime cyber operations. In the United States, peacetime or prewar operations (beyond intelligence collection) are typically surgical, designed to strike a balance between achieving the desired impact while avoiding excessive effects that would trigger a harsh retaliation or compromise precious cyber capabilities. Such operations typically require a much higher degree of sophistication to strike this delicate balance: they are typically more limited in their scope, duration, and effects. When they are designed to convey signals, such operations are also spaced out to allow their messages to be noticed and internalized. The corollary of these observations also seems to hold true, namely that in wartime many of these requirements and constraints wither away.

Yet the Russian modus operandi in Ukraine reveals a different overall attitude toward peacetime operations. Many Russian operations have been compromised or at least neutralized before they could inflict serious damage.[19] This rather underwhelming track record can in part be traced back to Ukraine's growing sophistication—and that of their national and corporate Western backers—in exposing and dealing with such Russian infiltrations. Russian sloppiness (and high tolerance for failure) in cyber operations could also partially explain the dismal record. But it is also plausible that part of the explanation resides with the logic guiding at least some Russian operations. Simply put, we also have to allow for the possibility that Russian operators may be seeking not physical impact on their Ukrainian adversaries but rather persistent harassment both before and during the armed conflict. Russian operations might have also been motivated less by the expected effects on Ukraine and more by domestic political or institutional imperatives to display action. In the absence of intimate knowledge of Russian thinking, definitive explanations of Russian performance elude us; the tentative impression is that we are likely witnessing a mixture of all the above factors. But going forward we may need to consider the possibility that Russia and others may undertake peacetime offensive cyber operations aimed at strategic harassment and that they may assess the desirability and utility of such operations based on criteria (or Measures of Effectiveness) that are divorced from their immediate prospects of producing tactical effects.

Russian employment of offensive cyber operations (like its behavior in many other realms) differs from the U.S. and more broadly Western approach in one additional operational respect: Russia seems to care far less about blowback from its offensive cyber operations, let alone revelations about its cyber conduct. Russian officials are content to flatly deny accusations and demand their accusers produce hard evidence, knowing that it is unlikely to

come. Western powers, on the other hand, appear to tread more cautiously in this space both operationally and publicly. Although they do not typically acknowledge specific offensive operations, when such activities are exposed they rarely deny having undertaken them, occasionally even leaking or alluding to such actions to reap political, institutional, and deterrence benefits, including the benefits from cyber attacks attributed to them that they do not officially acknowledge. References to U.S. offensive actions in the war against ISIS as well as more circumspect recent statements pertaining to USCYBERCOM's "hunt forward" operations in Ukraine are cases in point.[20] Well-documented but not formally acknowledged cyber attacks widely believed to have been carried out by the United States and Israel against Iran's nuclear program (Operation Olympic Games), and more recently by Israel against Iran, seem consistent with this pattern.

But the differences between the United States and Russia in offensive peacetime cyber operations run even deeper than their modus operandi, significant as this is. Russian cyber operations in and over Ukraine between 2014 and 2022 fit a pattern of behavior already evident in their cyber campaign against the 2016 U.S. elections as well as against Estonia (in 2007 and again in 2022).[21] All reveal a consistent Russian pattern of employing various offensive cyber means in peacetime as political instruments of harassment, subversion, and/or coercion. Russia repeatedly employs such methods alongside more overt tools to project its influence and favorably shape the political environment. The United States largely eschews such practices in peacetime, especially in recent years.

In Wartime

Onset of a Shooting War Sidelines Offensive Cyber Operations

Whereas cyber warfare may take center stage in a prewar period, once hostilities turn into open military confrontation cyber warfare is relegated to an auxiliary role. Cyber cannot occupy territory, nor can it consistently kill and destroy at an industrial and scale. Its effects and blast radius are far less predictable than those of its kinetic equivalents. Even meaningful cyber gains are typically ephemeral, transient, and/or reversible. And they are also inherently less measurable and less visible than physical gains, and hence they have much less potential to mark progress, let alone provide a platform for domestic political leverage, unless they are consolidated and cemented by physical gains. These inherent limitations, which as Jon Bateman has compellingly illustrated have thus far been evident in Russian cyber operations in the Ukraine conflict, reinforce the conclusion that offensive cyber operations during an armed conflict are not strategically decisive. As a result, cyber means are only rarely the weapons of choice when kinetic weapons could be effectively employed. This view thus reflects and reinforces a widespread belief that once war starts, cyber weapons are relegated to an auxiliary role.

This muted assessment of cyber warfare does not downplay cyber's potential battlefield contribution in this auxiliary role. Offensive cyber tools can facilitate and complement kinetic operations by temporarily diverting attention, by incapacitating an adversary or throwing them off balance, or through other forms of intimidation. Yet it does suggest that in the broader scheme of things cyber impacts are dwarfed by those of kinetic operations and the latter remain the primary measure of success. This conclusion fits into a rich and long-standing theoretical debate that has arisen every time a significant new warfighting domain or novel capacity has emerged: whether that new domain or weapon system has revolutionized warfare or has become the dominant fact to be reckoned with in future conflicts (for example, airpower post–World War I). The debate has never been satisfactorily resolved (except perhaps for nuclear weapons): the bottom line is always that it depends on what metrics one employs to measure the new domain's contribution, an issue we shall tackle below.

The Nature of Offensive Cyber Operations Evolves Over Time

Cyber encounters precede the escalation into open hostilities, continue once hostilities have broken out, and often persist after they end. Yet, a fundamental transformation in their very nature nevertheless occurs once open hostilities begin, as cyber operations then become part and parcel of far broader overt military and political warfare. This transition involves a significant shift in the role and modalities of the cyber component and its rules of engagement in the conflict, alongside a corresponding change in the role various institutions play in the conduct of cyber warfare in the military theater of operations. With war underway the need to exercise great caution, secrecy, compartmentation, and cover in offensive cyber operations dwindles. Higher visibility becomes the reality for cyber operations occurring in both offensive and defensive operations.[22] Gavin Wilde illustrates this evolution in his analysis of Russian cyber operations in Ukraine.[23]

The Challenges of Effective Coordination and Synchronization Between Kinetic and Cyber Operations

Jon Bateman analyzes in some depth claims that have been made, especially by Microsoft, that Russian cyber fires in Ukraine have been frequently coordinated and synchronized with their military operations.[24] He finds little evidence to substantiate such claims, with the notable exception being the Viasat hack. Some evidence might still surface warranting modification of this conclusion. But even if it does not, some may still argue that the Russian failure (or unwillingness) to coordinate such campaigns is sui generis, attributable to a unique set of actors and circumstances.

Nevertheless, our contention is that the Ukrainian case attests to generic challenges that stand in the way of integrating offensive cyber operations into warfare. To enhance the likelihood that they produce the desired effects while avoiding undesirable ones, offensive cyber operations must be tightly integrated with overall war plans: operationally, temporally,

geographically, and above all functionally. Yet such integration across so many dimensions is especially challenging and constraining. It often requires interagency (and sometimes, as in Ukraine, inter-proxy) coordination and overcoming organizational and parochial barriers.[25] Especially tight secrecy and compartmentation were imposed on Russian President Vladimir Putin's decision to go to war and its timing, which seems to have had an adverse effect on overall Russian performance in every domain, well beyond cyberspace.[26] The tight coupling requirement also produces other unwelcome side effects. Cyber war plans cannot be adjusted rapidly to changing circumstances on the battlefield without compromising their precision, efficacy, and predictability in achieving their intended results. Furthermore, tight coordination also means that the otherwise desirable compartmentation and secrecy regarding cyber operations would have to be relaxed, and the other way around, thereby significantly raising the prospect of premature compromise of either or both.

Cyber Versus Electronic Warfare

Once fighting actually breaks out, combat cyber means become part of a comprehensive effort to monitor, interfere with, and protect electronic signals transmissions, reception, interpretation, and exploitation.[27.] Our understanding of developments in this realm in Ukraine still leaves much to be desired. Yet from what we can glean from the available evidence, the advent of cyber has not caused the Russians to drastically modify their classical doctrine and corresponding force structure in this realm. They continue to assign a far higher priority to electronic warfare operations over cyber. In addition to stationary strategic electronic warfare contingents, Russia also relies heavily on mobile operational and tactical electronic warfare units to accompany and operate alongside all major deployed formations.

The role Russia assigns to electronic warfare stands in sharp contrast to the U.S. approach that neither assigns electronic warfare the lead role in the electromagnetic realm nor deploys massive electronic warfare contingents to accompany its deployed forces. It is practically impossible to assess for now which of these operating models is superior, though the partial evidence presently available suggests that the Russian electronic warfare units have fared no better than the remainder of the deployed invading forces in the early stages of the war. Russian electronic warriors have been impactful in jamming conventional Ukrainian military communications on the front lines; they have also employed direction-finding capabilities in support of targeting later in the war once the battlefront became more fixed. Either way, lessons pertaining to the electronic warfare dimension may have relevance for other militaries emulating the Russian approach.

Cyber Warfare as a Component of Reflexive Control

One prominent area in which the Russian attitude toward cyber operations differs markedly from that of its Western counterparts is in its emphasis on manipulating the thinking and behavior of not only its foes but also its own citizens and other pertinent parties. This

approach is derived from the well-entrenched half-century-old Russian theory of "reflexive control."[28] This theory, which long predates the emergence of cyberspace and tools, now weaves together cyber operations with censorship, propaganda, disinformation, public relations, and even diplomacy. More recently, General Valery Gerasimov has elevated the theory into a strategic doctrine that accords information operations no lesser importance in shaping the battlefield than conventional firepower.[29]

Whereas Western powers generally conceive of cyber operations as primarily creating effects either on or through digital systems, the Russian strategic doctrine treats cyber operations as akin to what the Chinese refer to as "informatized warfare."[30] And, as Gavin Wilde has pointed out, this conception of the information campaign reflects a far broader vision of the confrontation than is common in the West, as it views securing narrative dominance as a key component of comprehensive and top-down "society-centric warfare," at the heart of which lies an attempt to manipulate and redefine Ukranian identity along cultural, political, and religious dimensions.[31]

Indeed, the Ukrainian conflict provides some preliminary insights into how reflexive control theory is implemented in the context of a major and protracted war. Consistent with this doctrine, Russia is undertaking a massive information and influence campaign directed at a wide range of audiences: at home, in Ukraine, in Europe, and even in Asia and Africa. This campaign has seen some success in rallying support for Russia's war effort both domestically and abroad, suppressing dissent and organized resistance to its miliary occupation, and denying Ukrainian and Western efforts to impact these primary audiences.

The cyber component is thus part and parcel of a broad information campaign that, as Gavin Wilde and Justin Sherman explained, Russia seems to view as another means of advancing its overall agenda of regime survival against domestic and foreign conspirators.[32] Other instruments harnessed for the same goal include intelligence, kinetic and electronic warfare attacks, public relations and propaganda efforts, censorship, repressive internal security measures, disinformation, and diplomacy, partially reinforced by various forms of foreign aid. Taken together they serve to intimidate, harass, subvert, discredit, undermine, and incapacitate the regime's domestic and foreign foes, weakening and sowing discord among them while wooing and empowering Russia's supporters, allies, and partners.

The role assigned to cyber in this effort is to corrupt and disrupt communications, as well as to compromise unfavorable messaging by other parties while injecting its own. It seems that the prominence Russia is assigning to these goals has de facto made them into one of the two primary missions of its cyber apparatus, the other, of course, being intelligence collection. It flows naturally from this logic that the Russian leadership has assigned the execution of this function in cyberspace to its leading state security organ, the Federal Security Service (FSB), which retains the overall authority to coordinate all instruments available to the state to safeguard its internal security (which, remarkably, Russia interprets as including Ukraine).

At a higher level of abstraction, what the Ukraine case reveals is that Russia is marshalling all the means at its disposal, cyber included, to conduct a society-centric campaign.[33] This campaign has thus far proven to be far more successful inside Russia than in the areas it has occupied or targeted in Ukraine or Western Europe and has yielded mixed results elsewhere in the world.[34] Importantly, though, while Russian conduct in the Ukrainian conflict manifests some unique and context-specific characteristics, we should anticipate that other regimes will emulate such an approach and apply it elsewhere.

This is where the Russian, Chinese, and Iranian attitudes (to name just a few salient examples) toward cyber operations contrast so sharply with the contemporary Western one. While Western nations historically have rarely shied away from employing overt, covert, and military means to shape the political order in foreign lands and occasionally even at home, they have more recently come to consider covert actions in this realm as illegitimate domestically and dubiously legitimate abroad (as well as possibly ineffective), certainly in peacetime.[35] Yet Russia, China, Iran, and other non-Western nations do not seem to share such reticence.[36] And in a remarkable manifestation of mirror imaging, they all ascribe similar practices and motivations to Western nations.

Yet democratic nations now seem largely content to confine the remit for their nonwartime influence operations to overt means and public diplomacy abroad and defensive cyber missions (carried out mostly by dedicated cybersecurity agencies) domestically. The same can hardly be said of their nondemocratic rivals. This largely explains why in the latter the remit for undertaking these operations resides first and foremost in their internal security agencies—a choice that clearly has a bearing on these nations' institutional choices, doctrine, and human resource allocation, as well as their willingness to use proxies to carry them out.

Lifting the Fog of War

War has long been viewed as a chaotic and unpredictable encounter, in which the protagonists are all afflicted by various degrees of uncertainty and confusion over the situation on the battlefield let alone its likely outcome. The Ukraine war shows that technological developments coupled with massive investments in early warning and situational awareness tools and capabilities, not least in the realms of cyber, artificial intelligence, and data fusion, have yielded significant benefits in understanding the situation on the ground and anticipating immediate developments. What stands out in the Ukraine conflict, however, is that Ukraine and its Western allies have fared much better than Russia in the competition over cyber defense, early warning, battlefield situational awareness, and targeting information. This is due in large part to the richness and sophistication of the technical capabilities brought to bear by the U.S. and UK governments as well as various commercial entities (including SpaceX, Palantir, Microsoft, Amazon, Mandiant and many others), some of which received funding

from the U.S. and UK governments.[37] These actors came to Ukraine's help with intelligence as well as invaluable space reconnaissance sensors, telecommunications, and other technical assets and capabilities for fusing information and deriving operational cues. The Ukrainians skillfully wove these assets together with their indigenous resources.

However, it is important to distinguish between the capacity to greatly improve situational awareness though sophisticated fusion of diverse digital sensors and the ability to anticipate the outcome of encounters on the battlefield and beyond. Remarkable Western/Ukrainian progress in lifting the fog of war has not made it possible to anticipate outcomes, given the enduring significance of variables and developments outside cyberspace that remain hard to observe, measure, and predict, such as leadership and societal behavior.

Technical and Commercial Developments Degrade the Capacity to Seal Off the Cyber Battlespace to External Interventions

Attackers seek to cordon off the battlespace both virtually and physically in order to implement their war plans with as little disruption as possible. In physical space this is often done through a combination of restraint and deterrence that diminishes external parties' motivations to intervene as well as through active measures that limit their capacity to do so. As the Ukraine conflict makes abundantly clear, however, such a cordon is extremely difficult to impose in the cyber dimension. It is likely to prove even more challenging when third parties of all kinds find more opportunities to support one of the protagonists and/or to seize on other opportunities presented by the conflict.

The Ukraine conflict is instructive on one additional aspect of cordoning the digital battlespace. As has been observed, the digital domain of a protracted conflict is particularly likely to spill over beyond the territory of the immediate protagonists. Some of this expansion of the zone of conflict might be the result of unintended leakage; however more probably some protagonists or their sympathizers are consciously choosing to expand their area of operations to target their adversaries' exposed assets, undermine their support and external supply chains, deter external parties from getting more heavily involved, or possibly to draw them in. Given the global and interconnected nature of the digital world, odds are that a local conflict, even when it remains physically concentrated in a relatively well-defined geographic war zone, could nonetheless spread digitally around the world, and the probability that this would happen would keep on growing the longer active hostilities continue.[38] Unsurprisingly, Microsoft Threat Intelligence has indeed documented how Russia's cyber warriors have greatly expanded their activities against the United States, as well as Central and Eastern European targets since late 2022 and even more so in early 2023.[39] Other observers concur with this assessment, seeing concrete evidence that in recent months Russia has dramatically scaled up its cyber intelligence operations against Western and Eastern

European targets.[40] There is still some uncertainty whether these operations are primarily driven by information collection requirements and/or intended to deter or create retaliatory options. These observers deem it likely that Russia will further expand the digital battlespace beyond Ukraine should it face serious, additional setbacks in the conventional military realm.[41]

The prospects of cyber contagion are not solely related to the political proclivities and core interests of the specific parties but are also linked to some deep-rooted characteristics of the digital world. As the Stuxnet malware has already demonstrated, cyber attackers often lose some control over the exploits they employ. Nor can they necessarily contain the dynamics that certain offensive cyber activities may unleash. These spillover effects might in turn expand the conflict beyond its kinetic geographic boundaries (as was the case in the Ukraine conflict with the Viasat hack).[42] Such leakage or spillover, already apparent in the kinetic domain with the leakage of some conventional arms that have been provided by Western powers to Ukraine, can happen much faster and more widely in the cyber domain, unleashing unintended and undesirable consequences.

Some additional implications flow from this analysis. For instance, it raises the question of whether, although it is not possible to cordon off the entire digital battlefield, it might be feasible to (selectively) seal off parts of it, however temporarily. For example, electronic warfare could block (or spam) at least some frequency range of the spectrum for a certain duration.

In the final analysis the contagion effects and the growing difficulty of cordoning off the digital battlespace introduce a great deal of complexity and uncertainty into planning and executing campaigns, while simultaneously making it more difficult to predict their outcome.

Saving One's Fire in War

One might expect wartime offensive cyber operations in and on the battlefield, like their conventional counterparts, to be massive, incessant, and heavily focused on disruption or destruction of the adversary's military usable assets, resources, and capabilities that could complicate attainment of the military mission. Yet as Jon Bateman has pointed out, in the Ukraine conflict we have not seen much of this happening beyond the first days of the war. Bateman offered several plausible explanations for this observable anomaly, including the unraveling of the original war plan, the lack of advance preparation, and the inherently limited and time-consuming process of regenerating sophisticated cyber attacks.[43] Any of these may explain the significant lulls in the scope of Russian offensive cyber activities.

But there is one more possible explanation that is worth noting, which is rooted in another important characteristic shared by cyber and conventional offensive operations: the imperative to refrain from unleashing all of one's offensive power at the outset. Cyber and

conventional offenses typically hold back some significant residual capacity as a hedge against uncertainty. Not only is it difficult to anticipate whether, when, and where the employment or deployment of these assets might prove necessary, protagonists also wish to deter the immediate adversary and those backing him and keep them worried about extra capability the protagonists may hold in reserve. For Russia in Ukraine, this motivation may well have been particularly compelling given its strong desire to dissuade Western powers from directly intervening in the conflict and preparing a response in case they do.

In the cyber domain, however, there is also a third motive for pacing one's offensive actions, namely a concern about the rapidly diminishing utility of tools once they have been fully exposed. Offensive cyber capabilities, unlike conventional ones, may not be additive, and they cannot be extensively reused once employed and exposed. In the absence of reliable inside information it is impossible to conclude whether any of these rather generic factors has actually had impact on the Russian offensive cyber operations in Ukraine. But going forward we must keep these possibilities in mind, as they may assume some importance in other conflicts as well.

Digital Networks Might Be Surprisingly Robust and Agile

One especially novel insight to emerge from the Ukraine conflict is the relative agility of digital infrastructure (telecommunications, computers, and data) compared to physical infrastructure. Physical, electromagnetic, and cyber attacks can undoubtedly disrupt and even destroy key digital assets and undermine or diminish the efficacy of the missions they serve. But Ukrainian digital infrastructure (especially its cell towers and data servers) has been able to absorb fairly massive Russian missile as well as cyber attacks and continue to function, notwithstanding some temporary setbacks. Some of this success may be attributed to Ukraine's prior experience with Russian cyber aggression as well as its advance preparations, which also benefitted from an early warning of an impending attack. Ukraine cyber defenders have also been able to draw extensively on foreign assistance from governments and corporations as well as significant local and expatriate Ukrainian cyber expertise and expatriate assistance.[44] On top of it all, it appears that modern digital technology networks (such as those based on mobile and satellite communications and cloud computing infrastructure) are more robust and resilient than older infrastructure, allowing relatively quick reconstitution, preservation, and repurposing of key assets and functions.

Fusion of Cyber and Space

Another relatively novel feature of the Ukraine conflict is the growing fusion between space and cyberspace and between the digital infrastructure on land and in space. Digital information, telecommunication, navigation, and mass communication assets are vital for modern warfare, and many now operate in or through space. In the Ukraine conflict we can detect early signs that attacking (and defending) space assets is not only deeply integrated

with warfare in the air, sea, and land but is also heavily intertwined with digital confrontation in other domains. Control (or conversely disruption or disablement) of digital assets in space is thus becoming indispensable to gaining the upper hand on the battlefield and in the overall war effort. Even more interesting, cyber and electromagnetic operations are emerging as preferred means of projecting might into space to gain an advantage in a campaign. This raises the intriguing question of whether the ownership of the space assets providing digital services to land warriors makes a difference. Does it affect their appeal as targets, for example when they are owned and operated by commercial versus state entities or by commercial entities of noncombatant states? The attack on Viasat as well as efforts in other conflicts to jam satellite communications suggests that for now commercial space assets, even those owned by noncombatants, are considered fair game if they provide services to any of the protagonists.

Pre-delegation, Mission Creep, and Indiscrimination Should Be Expected

Offensive cyber operations in conflict situations prior to the onset of war typically involve discrete, isolated attacks or series of attacks. These seem to be shrouded in a tight veil of secrecy and compartmentation and carefully vetted, even if the standards and processes for such vetting may leave a fair amount to be desired.[45] Once fighting breaks out, and especially when it continues for a while, the vetting process for such operations fundamentally changes. Pre-delegation of authority to conduct cyber operations occurs, remits are expanded, and additional parties partake in the exchanges. Some mission creep in the aims and means employed, and the targets engaged, seems almost inevitable in a protracted conflict.

The Ukrainian conflict may be telling a still larger story. It reveals a rather cavalier Russian attitude about causing indiscriminate damage, both in its conventional operations and its electromagnetic ones, cyber included. Russia's wanton use of artillery and other forms of attack in Ukraine (and earlier in Syria and the Caucasus) exemplifies this attitude. Such a lack of discrimination, evident in the prewar situation but far more profound once war broke out, may be rubbing off on Russia's cyber warriors. Given that Russia's primary cyber forces are housed in its intelligence agencies, Russia's intelligence culture may exacerbate cyber operators' willingness to employ brutal means to get results.[46] It could also be that Russian technological cyber shortcomings and intelligence (targeting) limitations preclude more precise targeting or that indiscriminate attacks reflect an outburst of frustration, rage, and war fatigue (which are often the cause of atrocities). More alarmingly, it might reflect a Russian belief that inflicting collateral damage can serve its war aims. Such damage is not unintentional, but rather a chosen means to intimidate adversaries, demonstrate resolve, and warn third parties to keep their hands off the Russian prey.

In the absence of firsthand knowledge, we are in no position to determine which of these reasons or what combination accounts for the observable outcome. But this situation leaves us at least for now with at least two significant takeaways. First, we have to allow for the

possibility that when engaging in warfare, non-Western cyber powers, because of capacity limitations, indifference, or conscious choice, might be far more aggressive (in choice of targets) and indiscriminate (in causing effects) in their offensive cyber operations than is customary in the West. Second, we must also appreciate that more liberal rules of engagement for offensive cyber warfare could unleash practitioners to engage in broader, more intensive, and potentially far more escalatory cyber campaigns.

No Holds Barred?

Earlier we considered the evolving norms around what offensive cyber operations might be deemed an armed attack or an act of war. Now we ought to broaden this discussion to consider how the law of armed conflict (LOAC) as well as international humanitarian law (IHL) could apply to the question of which targets should be considered off-limits for offensive cyber operations. The extensive deliberations that have taken place over the years on cyber norms development (at the United Nations, around the *Tallinn Manual*, and in various ad hoc settings) have not formally codified which specific assets fall under the definition of critical civilian infrastructure that should not be attacked. An implicit consensus has emerged that purely civilian targets should be off-limits, along with a nominal consensus that critical infrastructure represents such a category and hence should be spared from cyber action.[47] But there have been no follow-up agreements, neither to formally codify which specific assets fall under this definition nor to establish caveats that may apply to the general prohibition on attacking them.[48]

Nevertheless, the examples cited in the United Nations Group of Governmental Experts (GGE) 2021 final report of critical infrastructure assets,[49] and any reasonable interpretation of the customary IHL restrictions in the physical domain, would lead to the conclusion that power plants (especially nuclear), heating and water plants, and critical information infrastructure certainly fall under the GGE norm. Purely civilian/humanitarian facilities such as hospitals, schools, and churches, along with their personnel, fall squarely under the IHL category of "specifically protected persons and objects"[50] and should be widely recognized to be off-limit targets for all military operations, presumably including cyber.

Yet in Ukraine such targets have been repeatedly subject to Russian conventional as well as cyber attacks, many of which also aimed at severing the communication lifelines servicing these facilities. In fact, as Alexander Baunov has pointed out, these attacks represent a premeditated effort to destroy all vestiges of infrastructure built by the Soviet Union in Ukraine, as a way of punishing the Ukrainian people for their resistance to the Russian onslaught.[51] Such attacks put in harm's way not only the staff and users of these facilities but also likely millions of innocent bystanders who depend on their safe and unimpeded functioning. This leads to the sobering conclusion that since no holds are barred in using conventional means to target civilian and even humanitarian facilities and personnel, as well as their essential auxiliary digital infrastructure, it is even more unrealistic to expect parties

to a bitter conflict to hold back from targeting and impacting such facilities by cyber means. After all, cyber attacks are widely believed to be far less destructive or permanently disruptive than their kinetic counterparts.

Although Russia's behavior has clearly been especially reckless and indiscriminate, it is prudent to anticipate that others in the future will similarly claim that their cyber attacks against such targets are perfectly legal. We should expect perpetrators of such attacks to argue, or even to genuinely believe, that cyber attacks against civilian targets during an international armed conflict meet the IHL criteria of being necessary, proportionate, and discriminate, as long as a legitimate case can be made that these targets also serve some military functions. Such targets could be argued to represent an effort to select what has been called "military objectives as well as means which may be expected to cause the least danger to civilian lives and civilian objects" as well as to minimize "incidental loss of civilian life, injury to civilians and damage to civilian objects."[52]

What holds true for Russia and possibly many other states certainly applies to their proxies, which typically demonstrate even less regard for cyber norms. This applies not merely to state-sponsored mercenaries such as the Wagner Group but also for patriotic nonstate warriors that nominally pursue legitimate causes. A case in point is the "IT Army of Ukraine," a hacktivist collective that takes its targeting cues from a state entity to conduct destructive attacks (albeit unsophisticated distributed denial of service [DDoS] attacks) on what Russia would consider civilian "critical infrastructure."[53]

The Salient Role of Proxies

Employing proxies as part of one's war effort has been a common practice for ages. In the Ukraine conflict it has been evident all along but became more pronounced once fighting evolved into open warfare: over Crimea in March 2014, in Eastern Ukraine's Luhansk and Donetsk regions since, and all over Ukraine as of late February 2022. Russia has been especially energetic in employing proxies, stretching the practice of plausible deniability beyond any credible limit in Crimea (recall the "little green men" in 2014) and elsewhere (for example, the Wagner Group's activities in Burkina Faso, the Central African Republic, Libya, Mali, and Syria). And its use of cyber proxies has been prolific.[54] But the Ukrainian government for its part has also been encouraging and supporting its volunteer IT army. Both parties have moved over time to officially integrate these fighting forces into their overall campaigns, with the vagaries of war gradually leading them to diminish their earlier efforts to nominally keep these entities at arm's length.

Tolerance, abetting, and actual recruitment of proxies to do one's bidding in conflict raises serious issues in every domain. Three are noteworthy in cyberspace. First, proxies amplify the challenge of integrating the cyber war (and warrior) into the overall war plan. Second, they greatly expand the prospect for extensive collateral damage perpetrated by players who are incapable of or disinterested in containing it. Finally, they raise the prospect of further

leakage of sophisticated exploits and tool chains from governments to these quasicommercial proxies (the equivalent of privateers) and from them onward to the criminal cyber community. The latter are especially ill-equipped to employ such tools responsibly or, perhaps even worse, may be eager to employ them liberally to enhance their intimidation and coercion clout.

Multinational Corporations Have Been Vital in Defending Ukraine

The leading technological platforms are huge, resourceful, sophisticated, influential, and global in scope. They provide vital telecommunications and data services as well as numerous applications. In Ukraine, as Nick Beecroft has pointed out, they have emerged as almost omnipotent independent players in the information scene and the cyber battleground.[55] Not only do their internal policies on who to assist, ignore, confront, or punish have a huge impact on the cyber confrontation itself, but they also wield considerable clout with governmental decisionmaking and possess remarkable resources to influence public opinion around the world. Such influence also extends to metanarratives about the role of cyber in conflicts and the necessity of norms to shape it.

Whether such external intervention by nonstate parties can be expected in other conflicts, however, remains an open question. Can such activity be sustained over time by corporations whose fiduciary requirement is, after all, to maximize profit? And for those pinning their hopes on such external interventions, a great deal depends on whether they can count on such support and whether they can engage in extensive advance contingency planning to enhance its impact when it happens.

How Should We Assess the Impact of Cyber Operations? What Are the Metrics of Success?

Perhaps the most vexing question scholars interested in cyber warfare have confronted is whether the introduction of large-scale cyber operations has made a profound impact on the battlefield and the conflict as a whole.[56] There are many obvious reasons why a definitive answer to this question eludes us at present and likely will for a long time, for the Ukraine war specifically and for warfare more broadly. Rather than join the emerging thoughtful debate, we consider here only two subsidiary questions: What criteria should one employ to assess cyber's impact on the conflict? And what broader conclusions are appropriate to draw from the Ukraine conflict?

Answers to these questions depend on what one wishes to accomplish through cyber operations and what one aims to avoid when authorizing and conducting them. On these issues the Ukraine conflict sheds light on a huge difference not only between nations but also between the various institutions engaged in such operations in terms of the role they assign to cyber operations and their expectations for those who carry them out.

The keys to effective defensive and offensive cyber operations are: delivering the *desired effects* on the *intended target,* at the *right time* and for the *sought-for duration*, *bounding these effects* and confining them to the intended target, and *avoiding spillover and contagion*, whether from the cascading effects of the attack, the exposure of the vulnerability exploited in the operation, the compromise of the tools and modalities used, or some combination of these. These parameters of success are of utmost importance in defining not only the operating space for cyber operations but also the level of dependence on (and resources allocated to) cyber operators. But the parameters are also clearly subjective, reflecting cultural, political, and institutional priorities and biases.[57] They may also be dynamic and context specific.

For example, Russia's priority of destroying or disabling targets regardless of collateral damage differs markedly from that of the United States, which considers surgical effects as well as limiting the proliferation of offensive cyber tools to be important metrics of success. Among other things this attests to the deep and enduring divide between democratic and nondemocratic states in their attitudes toward applying LOAC criteria of necessity, proportionality, and discrimination to cyber operations. Similar divergence is apparent in their aims and priorities for cyber operations. Apart from intelligence collection, which is a universal priority, the top priority for the cyber operators in nondemocratic regimes is to attain, sustain, and extend political control at home as well as over the theater of operations. This stands in sharp contrast to Western nations, the United States in particular, where the political control mission is more narrowly defined as denying the adversary the capacity to project its influence into one's domestic scene while projection of political control over the remainder of battlespace is far more narrowly defined to influence the military theater of operations. Conversely, battlefield support, which is USCYBERCOM's number one priority, is not only a secondary aim for cyber in Russia but is a role Russia mostly assigns to electronic warfare: it is electronic warfare units, not cyber units, that are closely integrated into the fighting units. From the perspective of these aims and priorities, Russian cyber performance in and around Ukraine may be assessed far more favorably.

There is also a sharp difference between parties not only in the role assigned to cyber operations but also their desired effects. Should they be primarily cognitive, as Russia and other nondemocratic states prefer, focused on intimidation and fear, confusion and paralysis? Or should they be more physically oriented, as is the general inclination in the West? And if physically oriented, should cyber operations be expected to produce temporary effects (disruption) or permanent ones (outright destruction or open-ended incapacitation)? It is noteworthy that in Ukraine, all the key parties have assigned cyber a disruptive rather than destructive role when seeking physical effects. Destruction, when sought, was assigned to kinetic operations, though these in some cases were preceded by cyber disruption. It is highly uncertain whether cyber will remain a primarily disruptive tool going forward and whether other nations involved in conflicts will also subscribe to such an approach.

One may employ several other metrics for assessing cyber success, including its cost-effectiveness, its unique contribution to warfighting, its surge potential, its versatility (especially when it comes to functional and/or geographical repurposing), and its force projection

capacity. The existing theoretical literature suggests that cyber scores well on many of these parameters. Yet so far, the publicly available empirical evidence from Ukraine does not immediately lead to the conclusion that offensive cyber operations have been an unqualified success there, notwithstanding its superior qualities in the abstract.

The Postwar Period

Although the Russia-Ukraine conflict has yet to reach a "postwar" status, we can speculate about some likely key lessons for postconflict cyber warfare there and elsewhere.

A Ceasefire Will Not End the (Cyber) Confrontation

Just as offensive cyber operations precede an armed conflict, so are they likely continue after it is suspended or over. In part this is because cessation of military operations in irredentist conflicts commonly constitutes little more than a fragile and temporary state. The Ukraine conflict stands out as a particularly sobering example of such a postwar scenario precisely because of the high stakes and level of antagonism for all the concerned parties, none of whom view this war as a local or transient affair. Putin (as well as many others in the Russian elite) has long defined Ukraine's status as germane to Russian identity and post–Cold War national security, while the war's outcome has now become inextricably tied to Putin's political fortunes.[58] Ukraine and its Western backers have conversely seen the conflict as far broader than Ukraine as such, viewing it as a most extreme challenge to the entire post–Cold War order in Europe and beyond (for example, Taiwan). When strategic interests, political considerations, and raw emotions combine and clash with those of the adversary, it is extremely unlikely that friction would end even when a ceasefire takes place. And this is precisely where employment of cyber means could look most appealing.

In such high-stakes conflicts, a ceasefire often represents little more than a transition from a phase in the conflict characterized by overt/lethal exchanges into a somewhat more subdued or transparent confrontation replete with persistent friction. In this phase, employment of cyber means would likely appear ideal for advancing the protagonists' immediate interests or at least helping them position themselves for a new chapter in the conflict. Cyber operations of varying intensity are thus extremely likely to continue (and might even be stepped up) against the adversary and its supporters in pursuit of signaling, deterrence, retribution, and influence. But other operations might be predominantly motivated by domestic considerations, not in the least to vent steam. Or they may use cyber to satisfy other parochial political (and institutional) interests, by inflicting disruptive and destructive effects on the adversary.

Defend Forward/Persistent Engagement Blurs the Dividing Lines Between Armed Conflict and the Postwar Period

Some of the bad blood after active warfare would likely come from a genuine disagreement over the legitimacy of certain types of cyber conduct (intelligence collection, defensive, offensive, and information operations) during a ceasefire or other de-escalation arrangement. But it seems extremely likely that in Ukraine (and probably many other conflict situations), a cessation of kinetic operations will not carry over into the information space. Especially intriguing in this context is the likelihood that offensive cyber operations will persist because of the presumed imperatives of the cyber domain, as well as the legitimacy that can be derived from the likes of the U.S. defend forward/persistent engagement doctrine.[59] This prospect is enhanced by the closely related reality that cyber operations carried out in adversary networks without their permission are not and probably will not be consensually codified as ceasefire violations.

Cover and Plausible Deniability Will Regain Prominence

Although offensive cyber operations are most likely to persist in a post-ceasefire environment, they are likely to change in one important respect. We should anticipate a much higher emphasis on concealing the identity of their true perpetrators (and those who stand behind them), as well as an increase in false-flag operations. The attitude and standards employed to conceal or assign responsibility for such operations vary greatly between the United States and Russia (and other countries). Regardless, it seems most likely that in postcrisis situations both parties (but especially Russia-like players) would assign malevolent intent and attribute offensive cyber ceasefire violations to the other party. And we should also expect those who undertake such operations to deny any culpability for the destabilizing impact of such conduct.

Key stakeholders' determination to sustain extensive cyber and information activities after the end of open hostilities is also likely to affect their goals and modalities. The most likely goal would be to preserve, undermine, or reshape the status quo in one's favor. In terms of modalities, we should expect an especially prominent role for false-flag operations, as well as extensive employment of proxies. In both cases the intent will be to blame the other party for the deterioration in stability, perhaps as a pretext for revisiting the situation frozen by the ceasefire agreement. Naturally, the involvement of one or more third parties in a conflict (as is the case in the Ukraine) greatly increases the odds that cyber means will contribute to confusion and genuine misunderstandings over cyber operations.

About the Author

Ariel E. Levite is a nonresident senior fellow in the Nuclear Policy Program and Cyber Policy Initiative at the Carnegie Endowment for International Peace.

Acknowledgments

I am hugely indebted to my colleagues at Carnegie's Technology and International Affairs Program for brainstorming together over the Ukrainian conflict's cyber dimensions as well as their invaluable insights, comments, and proposed edits on earlier drafts of this paper. Special thanks go to Peter Armstrong, Jon Bateman, James N. Miller, George Perkovich, Robert Schmidle, and Gavin Wilde for their many helpful suggestions. My thanks also to Isabella Furth for her editorial assistance. Obviously, I remain solely responsible for any remaining flaws in my analysis.

Notes

1 Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," Carnegie Endowment for International Peace, December 16, 2022, https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657; Nick Beecroft, "Evaluating the International Support to Ukrainian Cyber Defense," Carnegie Endowment for International Peace, November 3, 2022, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322; Gavin Wilde, "Cyber Operations in Ukraine: Russia's Unmet Expectations," Carnegie Endowment for International Peace, December 12, 2022, https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607; Microsoft Threat Intelligence, "A Year of Russian Hybrid Warfare in Ukraine," March 15, 2023, https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf.

2 The challenge is especially acute because we are unable to ascertain the veracity of what we think we know and do not know how much of the whole story it represents.

3 Indeed, a very recent study suggests that since January 2023, Russia has been regrouping for another round of massive cyber attacks against Ukraine. See Microsoft Threat Intelligence, "A Year of Russian Hybrid Warfare in Ukraine," March 15, 2023, https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf, 3; "Russian Hackers Are Preparing for a New Campaign in Ukraine," *The Economist*, March 29, 2023, https://www.economist.com/science-and-technology/2023/03/29/russian-hackers-are-preparing-for-a-new-campaign-in-ukraine. The rapidly shifting situation on the ground could be seen as a concrete illustration of Heisenberg's uncertainty principle, namely that the shape and very presence of observation can influence the outcome being observed.

4 For an insightful review of the evolution of Ukrainian cyber defense capabilities, see Gillian Tett, "Inside Ukraine's open-source war," *Financial Times*, July 21, 2022, https://on.ft.com/3cmQnKA.

5 A case can certainly be made that the conflict between Russia and Ukraine precedes 2014, as do Russian efforts to influence developments there. That said, there is no denying that the conflict escalated greatly once President Victor Yanukovych fled the country and Russia invaded and annexed Crimea. This makes 2014 an expedient starting point for this analysis.

6 For an extensive discussion of these operations by Russia see Bateman, "Russia's Wartime Cyber Operations."

7 An insightful perspective on this dimension of the Russian plan is provided by the *Financial Times*' one-year review of the lead-up to the war: Max Seddon, Christopher Miller, and Felicia Schwartz, "How Putin Blundered Into Ukraine — Then Doubled Down," *Financial Times*, February 22, 2023, https://on.ft.com/3KF3Uw2.

8 The March 2023 Microsoft Threat Intelligence report highlights the public-facing side of this practice, as well as the extensive Russian tapping of a "fifth column" in Ukraine: Microsoft Threat Intelligence, "A Year of Russian Hybrid Warfare," 7.

9 Remarkable insight into Russian intelligence and operations in Ukraine is provided in a *Washington Post* special report based on many captured documents and interviews: Greg Miller and Katherine Belton, "Russia's Spies Misread Ukraine and Misled Kremlin as War Loomed," *Washington Post*, August 19, 2022, https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war/.

10 An extensive discussion of the pertinent institutional and functional setup of Russian intelligence is provided in Wilde, "Cyber Operations in Ukraine." See also Seddon, Miller, and Schwartz, "How Putin Blundered Into Ukraine."

11 Some highly pertinent work related to this issue is taking place in the ongoing *Tallinn Manual 3.0*. However, we have to bear in mind this forum's inherent limitation, in that its national composition affects the broader appeal of its recommendations. The multiyear discussions in the UN GGE as well as the Open-ended Working Group (OEWG) also attest to the difficulty of reaching a broader international consensus on this issue.

12 An especially interesting case of disruption is the occupation by an "armed militia" of the server farm of a Ukrtelecom, the largest Ukrainian telecom network provider (March 2014). The captured assets were subsequently employed by the attackers to conduct a cyber attack throughout Ukraine, including on high-value targets. In this case, Ukrtelecom operating license provisions required it to be able to affirm at all times that there was no penetration of the network from alien technology. Yet the occupation of the data center meant the operator could no longer provide such an affirmation. Consequently, their operating license was suspended, which led to a significant business interruption claim that quickly evolved into a war exclusion argument. Two key points in this episode offer important generic insight into cyber warfare. One is the synergistic effects of physical and digital operations, the other is the difficulty of estimating the effects of a specific cyber attack in advance, due to the variety of factors that could affect its magnitude and severity. The latter point is underscored by a follow up Russian cyber attack on Ukrtelecom that took place after the start of the war. For details on this attack see Prateek Jha, "Ukraine's Largest Telecom Company Hit by Major Cyberattack," VPN Overview, May 4, 2022, https://vpnoverview.com/news/ukraines-largest-telecom-company-hit-by-major-cyberattack/.

13 For decisions on this matter taken at the June 2022 NATO summit, see Jennifer Hansler, "NATO Agrees Cyberattacks Could Amount to Armed Attacks and Lead to Invocation of Mutual Self-defense Clause," CNN, June 14, 2021, https://edition.cnn.com/world/live-news/biden-nato-summit-updates-06-14-2021/h_ea34b1915ddd061d6060d9f2da7417fe.

14 The preceding discussion has already alluded to the subjective definition of "success" in cyber operations: Is it hitting and impacting the correct target? Avoiding collateral damage? Making it difficult if not impossible to replicate or leverage the attack? These issues will be revisited in some depth later in this essay.

15 An explanation and illustration of the Lockheed Martin Cyber Kill Chain model can be found here: "The Cyber Kill Chain®, Lockheed Martin, accessed March 21, 2023, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

16 A concise and useful official summary of Russian cyberattacks against Ukraine in the lead-up to 2014 can be found in the U.S. Army's Cyberspace Operations Field Manual: Department of the Army, *Cyberspace Operations and Electromagnetic Warfare*, FM 3-12 (Washington, DC: Department of the Army, 2021), 2-2, https://rdl.train.army.mil/catalog-ws/view/100.ATSC/12BAB5E3-1C00-4DB8-B324-2AA7C6F6F420-1492095745021/fm3_12.pdf.

17 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *WIRED*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

18 A comprehensive review of the attack on Ukraine's electric grid can be found in Donghui Park and Michael Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks," Henry M. Jackson School of International Studies, University of Washington, October 11, 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/. An extensive description of Operation Olympic Games is provided by David E. Sanger in his book *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018).

19 See Bateman, "Russia's Wartime Cyber Operations," for an analysis of the efficacy of Russian cyber operations in Ukraine and his overall conclusion about their limited impact.

20 USCYBERCOM typically portrays its operations in adversary networks as predominantly defensive and undertaken in the context of the US Department of Defense's defend forward strategy. For the U.S. actions against IS, see Dina Temple-Raston, "How The U.S. Hacked ISIS," NPR, September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis. For USCYBERCOM statements regarding "hunt forward" operations, see General Nakasone's interview with Sky News: Alexander Martin, "US Military Hackers Conducting Offensive Operations in Support of Ukraine, Says Head of Cyber Command," Sky News, June 1 2022, https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139. See also Shannon Vavra, "U.S. Cyber-Offensive Against ISIS Continues, and Eyes Are Now on Afghanistan, General Says," Cyberscoop, September 17, 2019, https://cyberscoop.com/isis-jtf-ares-cyber-offensive-afghanistan/.

21 Andrius Sytas, "Estonia Says It Repelled Major Cyber Attack After Removing Soviet Monuments," August 18, 2022, https://www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber-attack-after-removing-soviet-monuments-2022-08-18/.

22 Lennart Maschmeyer's "Subversive Trilemma" is a great examination of these shifting modalities: Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," *International Security* 46, no. 2 (2021): 51–90, https://doi.org/10.1162/isec_a_00418.

23 Wilde, "Cyber Operations in Ukraine."

24 Bateman, "Russia's Wartime Cyber Operations."

25 In the Ukrainian conflict, Russia seems to have encountered a serious difficulty in coordinating the cyber efforts of multiple entities including the Federal Security Service (FSB), the National Guard of Russia, the Russian Ministry of Defense, the GRU, and the Wagner Group.

26 The *New York Times* investigation of the causes of the abysmal Russian military performance in Ukraine is very telling in this respect: Michael Schwirtz, Anton Troianovski, Yousur Al-Hlou, Masha Froliak, Adam Entous and Thomas Gibbons-Neff, "Putin's War: A *Times* Investigation Based on Interviews, Intercepts, Documents, and Secret Battle Plans Shows How a 'Walk in the Park' Became a Catastrophe for Russia," *New York Times*, December 16, 2022, https://www.nytimes.com/interactive/2022/12/16/world/europe/russia-putin-war-failures-ukraine.html. The *Financial Times* offers even more insights into the tight compartmentation of the war planning: Seddon, Miller, and Schwartz, "How Putin Blundered Into Ukraine."

27 For an interesting review of the Russian electronic warfare campaign in Ukraine, see Bryan Clark, "The Fall and Rise of Russian Electronic Warfare," IEEE Spectrum, July 30, 2022, https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare

28 Wilde's "Cyber Operations in Ukraine"discusses the doctrine of reflexive control in the context of Ukraine. Another piece which describes the application of reflexive control in the Ukraine conflict is Alya Shandra, "A Guide to Russian Propaganda. Part 5: Reflexive Control," Euromaidan Press, March 26, 2020, https://euromaidanpress.com/2020/03/26/a-guide-to-russian-propaganda-part-5-reflexive-control/.

29 Christian Kamphuis, "Reflexive Control," Militaire Spectator, June 21, 2018, https://militairespectator.nl/artikelen/reflexive-control.

30 For succinct reviews of the way China generally and the PLA specifically view informatized warfare, see Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, "People's Liberation Army Operational Concepts," Rand Corporation, 2020, https://doi.org/10.7249/RRA394-1; and Klon Kitchen, "Informatized Wars: How China Thinks About Cyber," The Dispatch, April 21, 2022, https://thedispatch.com/newsletter/current/informatized-wars-how-china-thinks/.

31 For a discussion of the contours and historical evolution of society-centric warfare see Ariel E. Levite and Jonathan (Yoni) Shimshoni, "The Strategic Challenge of Society-centric Warfare," *Survival: Global Politics and Strategy* 60, no. 6 (2018): 91–118, https://doi.org/10.1080/00396338.2018.1542806.

32 Gavin Wilde and Justin Sherman, "No Water's Edge: Russia's Information War and Regime Security," Carnegie Endowment for International Peace, January 4, 2023, https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644.

33 See Jonathan Shimshoni and Ariel E. Levite, "The Russo-Ukrainian War's Dangerous Slide Into Total Societal Conflict," The Buzz (blog), *The National Interest*, May 13, 2022, https://nationalinterest.org/blog/buzz/russo-ukrainian-war's-dangerous-slide-total-societal-conflict-202396; and Ariel E. Levite, "Finding a Way Out of the Societal War Over Ukraine," *The National Interest*, January 29, 2023, https://nationalinterest.org/feature/finding-way-out-societal-war-over-ukraine-206162.

34 For discussion of the Russian propaganda campaign in eastern Ukraine see "Research Exposes Long-term Failure of Russian Propaganda," University of Cambridge Research News, May 3, 2022, https://www.cam.ac.uk/research/news/research-exposes-long-term-failure-of-russian-propaganda-in-ukraines-donbas-region.

35 An instructive case in point is provided by the ebb and flow of U.S. influence campaigns in Venezuela. See W. J. Hennigan, "Inside John Bolton's Month-Long P.R. Campaign Against Venezuela's Government," *Time*, January 30, 2019, https://time.com/5516920/inside-john-boltons-month-long-p-r-campaign-against-venezuelas-government/; Ana Vanessa Herrero and Samantha Schmidt, "U.S. Outreach to Venezuela Strengthens Maduro, Sidelines Guaidó," *Washington Post*, March 11, 2022, https://www.washingtonpost.com/world/2022/03/11/venezuela-maduro-guaido-us-visit/; and Adam Taylor and Ana Vanessa Herrero, "John Bolton Said He Planned Foreign Coups. The Global Outcry Was Swift," Washington Post, July 13, 2022, https://www.washingtonpost.com/world/2022/07/13/john-bolton-coup-backlash/.

36 For discussion of repeated Iranian efforts to sow distrust and discord in Israel's elections see Nir Devori, "'It Works Without People Understanding': The Iranian Attempt to Influence the Elections in Israel" (in Hebrew), N12 Magazine, August 18, 2022, https://www.mako.co.il/news-n12_magazine/2022_q3/Article-cc76fcdb8f26281026.htm.

37 See Beecroft, "Evaluating the International Support to Ukraine." For SpaceX, see Mike Wall, "1,300 SpaceX Starlink Terminals With Ukraine's Military Went Offline Due to Funding Shortfall," Space.com, November 8, 2022, https://www.space.com/ukraine-spacex-starlink-terminals-offline-funding-shortfall; for Palantir: David Ignatius, "How the Algorithm Tipped the Balance in Ukraine," *Washington Post*, December 19, 2022, https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/; for Amazon: "Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future," Amazon, June 9, 2022, https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future; for Mandiant: "Ukraine Crisis Resource Center," Mandiant, accessed March 21, 2023, https://www.mandiant.com/resources/insights/ukraine-crisis-resource-center; for Microsoft: Brad Smith, "Extending Our Vital Technology Support for Ukraine," Microsoft, November 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/.

38 One issue to reflect on going forward is whether the human and technological strain associated with continuous high-intensity conflict increase the likelihood that the conflict's theater of operations in the digital domain will expand quantitatively, geographically, and even qualitatively—or whether, conversely, growing battle fatigue and resource constraints will actually diminish the prospects of such spillover.

39 Microsoft Threat Intelligence, "A Year of Russian Hybrid Warfare," 3.

40 "Russian Hackers Are Preparing," *The Economist*.

41 Microsoft Threat Intelligence, "A Year of Russian Hybrid Warfare," 17; "Russian Hackers Are Preparing," *The Economist*.

42 Matt Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine," *WIRED*, March 23, 2022, https://www.wired.com/story/viasat-internet-hack-ukraine-russia/.

43 Bateman, "Russia's Wartime Cyber Operations."

44 For the first official acknowledgement of the United States' contribution to Ukrainian cyber defense by a "hunt forward" operation, as well as the scope of Russian cyber attacks, see this review of General Paul Nakasone's talk at the Vanderbilt conference: Suzanne Smalley, "Nakasone Says Cyber Command Did Nine 'Hunt Forward' Ops Last Year, Including in Ukraine," Cyberscoop, May 4, 2022, https://cyberscoop.com/nakasone-persistent-engagement-hunt-forward-nine-teams-ukraine/. For a review of Microsoft's support of Ukraine, see Sean Endicott, "Microsoft Has Committed Over $35 Million to Help Ukraine," Microsoft Windows Central, March 23, 2022, https://www.windowscentral.com/microsoft-has-committed-over-35-million-help-ukraine; for Amazon's support, see "How Amazon Is Assisting in Ukraine," Amazon, December 1, 2022, https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine; for more on SpaceX's Starlink see Vincet Veritas, "Starlink Is Keeping Ukraine Connected to the World," Groundstation, March 25, 2022, https://www.groundstation.space/the-story-of-starlink-for-ukraine/. A good review of the Ukrainian cyber defense campaign can be found in Tett, "Inside Ukraine's Open-source War."

45 The United States, which is somewhat transparent about its vetting process for such operations, went through a significant liberalization of its rules of engagement in offensive cyber operations in 2018, when it revised Presidential Policy Directive 20 (PDD-20). See Mack DeGeurin, "U.S. Silently Enters New Age of Cyberwarfare," *Intelligencer* (blog), *New York Magazine*, September 11, 2018, https://nymag.com/intelligencer/2018/09/us-rescinds-ppd-20-cyber-command-enters-new-age-of-cyberwar.html.

46 For an interesting discussion of the Russian intelligence modus operandi that draws a comparison to Chinese intelligence statecraft, see John Paul Rathbone and Demetri Sevastopulo, "'On a Par With the Russians': Rise in Chinese Espionage Alarms Europe," *Financial Times*, August 29, 2022, https://on.ft.com/3pXi8wZ.

47 For an enlightening contemporary discussion on the evolution of the critical cyber infrastructure and the norms governing its protection, see "Critical Infrastructure," GIP Digital Watch, accessed March 21, 2023, https://dig.watch/topics/critical-infrastructure.

48 See especially Customary IHL Rule 7, which outlines the required distinction in military engagement of targets and the prohibition on directing attacks against civilian objects: "Rule 7. The Principle of Distinction Between Civilian Objects and Military Objectives," International Humanitarian Law Databases, accessed March 23, 2023, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule7.

49 The most explicit reaffirmation of the norm in this realm appears as Norm 13 (f) of the GGE final report adopted on May 28, 2021. It states that "a State should not conduct or knowingly support [Information and Communications Technology] activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." UN Group of Governmental Experts, Report A/76/135, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, May 28, 2021, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

50 For an ICRC description of IHL treatment of these targets, see Jean-Marie Henckaerts and Louise Doswald-Beck, "Specifically Protected Persons and Objects," in *Customary International Humanitarian Law, Part II* (Cambridge University Press, 2012), https://www.cambridge.org/core/books/abs/customary-international-humanitarian-law/specifically-protected-persons-and-objects/1ADE292CA15804EB3A9EB176D8957ADA.

51 Alexander Baunov, "Putin Is Launching an Assault on the Last Vestiges of Soviet Identity," *Financial Times*, January 22, 2023, https://on.ft.com/3XL5rVr

52 Jean-François Quéguiner, "Precautions Under the Law Governing the Conduct of Hostilities," *International Review of the Red Cross* 88, no. 864 (December 2006), https://www.icrc.org/en/doc/assets/files/other/irrc_864_queguiner.pdf, 805; "Rule 17. Choice of Means and Methods of Warfare," International Humanitarian Law Databases, accessed March 30, 2023, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule17.

53 Stefan Soesanto, "The IT Army of Ukraine: Structure, Tasking, and Ecosystem," Center for Security Studies (CSS) at ETH Zürich, June 2022, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf.

54 The latest Microsoft report documents and illustrates some of this practice. See Microsoft Threat Intelligence, "A Year of Russian Hybrid Warfare," 14.

55 Beecroft, "Evaluating the International Support to Ukraine." For stories on the role played by Microsoft, Amazon, and Starlink in enhancing Ukraine's cyber robustness and resilience, see Smith, "Extending Our Vital Technology Support"; "Safeguarding Ukraine's Data"; and Wall, "1,300 Starlink Terminals."

56 For a highly stimulating analysis of this issue that employs a creative approach to measuring impact, see Bateman, "Russia's Wartime Cyber Operations." Also of interest is Lennart Maschmeyer and Myriam Dunn Cavelty, "Goodbye Cyberwar: Ukraine as Reality Check," *Policy Perspectives* 10, no. 3 (May 2022), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-3_2022-EN.pdf. Dave Aitel and others offer some fascinating discussion of Maschmeyer and Cavelty's propositions in in Dave Aitel et al., "Goodbye Cyberwar," Google Doc, accessed March 23, 2023, https://docs.google.com/document/d/13ef8fOXtXW8v7m-Kc-IWPrhrAT07XfeZCGYO6azLsIo/edit.

57 What comes to mind here is a deeply ingrained Russian attitude captured by former Russian prime minister Viktor Chernomyrdin, who is quoted as saying, "We tried the best but it just turned out as always": AZQuotes, accessed March 23, 2023, https://www.azquotes.com/quote/803647.

58 A highly instructive official representation of President Putin's thinking on Ukraine was provided in his July 2021 official manifest, posted on the Kremlin's website. A useful annotated summary of its pertinent highlights can be found in "Every Russian Soldier Is Required to Read This 2021 Putin Article on Ukraine," Anti-Empire, January 16, 2022, https://anti-empire.com/every-russian-soldier-is-required-to-read-this-2021-putin-article-on-ukraine/.

59 For an extensive articulation of this imperative as the theoretical underpinning for USCYBERCOM's persistent engagement doctrine see Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford University Press, 2022). The doctrine itself is best encapsulated in Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs*, August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity#author-info.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers around the world. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Technology and International Affairs Program

The Carnegie Technology and International Affairs Program (TIA) helps governments and industries reduce large-scale international risks of new technologies and related services. Recognizing that commercial actors control many of the most germane technologies, TIA identifies best practices and incentives that can motivate industry stakeholders to pursue growth by enhancing rather than undermining international relations.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org