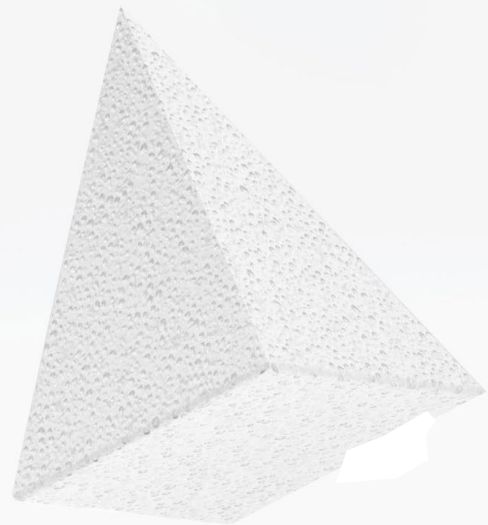
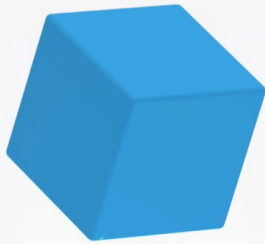
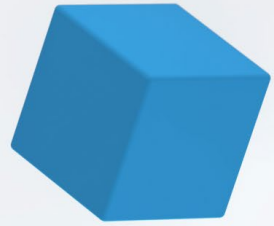


Cyber Effects in Warfare: Categorizing the Where, What, and Why

Jason Healey



For decades, military practitioners and academics have come up with theories, evidence, and examples that indicate that offensive cyber operations might revolutionize modern warfare. Others have made an equally impressive case that refutes that such operations would even be relevant, making it hard to reach any definite conclusions. This paper introduces a novel analytical framework to assess offensive cyber operations based on the circumstances of their use across the different phases of war, from shaping operations prior to the conflict to the actual battlefield. This framework substantially simplifies the key questions of practitioners and academics in order to pose the more direct question: Where, when, and how might offensive cyber operations affect warfare outcomes, both today and in the future?

Within 15 years of the invention of powered flight, nearly all of the doctrinal missions of an air force had been not just discovered but integrated under a single commander in battle: Billy Mitchell at the 1918 battle of Saint-Mihiel.¹ The pressure of extended high-intensity combat drove innovations in the use of airpower that were hard to imagine before World War I, when planes seemed fragile and of limited use on the battlefield. During that war, airpower started to come into its own, due to technological improvements, doctrinal advancements, and coordinated use by a single commander charged with integrating airpower with other combined arms to triumph in a major battle.

Adversaries in the full-scale invasion of Ukraine have similarly been pushing offensive cyber operations, discovering new relevance and missions — driven by those same pressures of combat — and hinting that there are more possibilities to come. Russia's invasion of Ukraine raises a critical question: Where, when, and how might offensive cyber operations impact the outcomes of war?

For over 40 years, answers to this question have been diverted into a debate of whether offensive cyber operations are revolutionary or mostly hype. While illuminating and important, much of that debate had to do with examining different aspects of warfare. It did not clearly differentiate between of-

fensive cyber operations that were conducted on an actual battlefield in the midst of a traditional tactical engagement between armed forces, those conducted well behind the front lines, and those conducted before the battle had even begun. Nor did it clearly specify if the target was a weapons system or not. Many assessments predated the full-scale Russian invasion of Ukraine and so lacked adequate examples of “cyberspace operations in a high-intensity interstate war,”² or an empirical base.³ Many were also based on incorrect assumptions — unstated, as often as not — that territorial conquest would be somewhat “anachronistic.”⁴

This article accordingly introduces a novel analytical structure to clarify the role of offensive cyber operations in warfare. The Framework for Offensive Cyber Operations in Warfare categorizes offensive cyber operations based on the circumstances of their use across the different phases of war, from pre-conflict shaping operations, to prior to the battle or in the rear echelon, to the actual battlefield. Within each of these three phases, offensive cyber operations can be categorized by intent: exploiting information, attacking information, attacking trust in weapons systems or critical infrastructure, and attacking weapons systems or critical infrastructure.

Not only does this framework contain appropriate examples for almost all of these 15 circumstances,

1 Rebecca Grant, “The Dawn of American Airpower at St. Mihiel,” *Air & Space Forces Magazine*, July 27, 2018, <https://www.airandspaceforces.com/article/the-dawn-of-american-airpower-at-st-mihiel/>.

2 “Lessons from Russia's Cyber-war in Ukraine,” *The Economist*, Nov. 30, 2022, <https://www.economist.com/science-and-technology/2022/11/30/lessons-from-russias-cyber-war-in-ukraine>.

3 Joshua Rovner, “Cyberspace and Warfighting,” in *Ten Years In: Implementing Strategic Approaches to Cyberspace*, Naval War College Newport Papers #45, 2020, ed. Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1044&context=usnwc-newport-papers>.

4 Nadiya Kostyuk and Erik Gartzke “Fighting in Cyberspace: Internet Access and the Substitutability of Cyber and Military Operations,” *Journal of Conflict Resolution* 68, no 1 (January 2024): 80–107, <https://doi.org/10.1177/00220027231160993>.



but many of the operations in these examples appear to have been tactically relevant and operationally successful. Most examples come from a single high-intensity war — the ongoing Russian invasion of Ukraine. Although these offensive cyber operations “have not achieved any systemic effects, and they have arguably been less cost-effective — or at least more capacity-constrained — than kinetic fires,” they indicate that states will use cyber capabilities in new ways during wartime.⁵

Framework for Offensive Cyber Operations in Warfare

Table 1 summarizes the Framework for Offensive Cyber Operations in Warfare, which categorizes operations by when or where the operation in question took place as well as by the intent of that operation. The framework begins by distinguishing the where and when of an attack, to better understand cyber operations conducted before hostilities versus those that take place just prior to a battle or behind the battle lines versus those used tactically during the battle itself.⁶ Many past analyses somehow failed to include this crucial criterion in their assessments.

The framework might in future be expanded to include offensive cyber operations that are related to a conflict but that take place outside of the zone of conflict (such as a Russian operation related to Ukraine but targeted at infrastructure in Europe or the United States).⁷ I have omitted this for now to keep the table a more manageable size.

The Framework for Offensive Cyber Operations in Warfare categorizes this when/where variable based on the intent of the operation, building on Daniel Moore’s useful characterization of operations as either presence-based — “strategic capabilities that begin with lengthy network intrusions and conclude with an offensive objective” — or event-based — directly activated tactical tools that can be deployed in the field to immediately create localized events.⁸ This framework includes five types of intent: *exploiting or targeting information, networks, and systems* (such as stealing or deleting information); *targeting trust*

in institutions or eroding morale (such as with cyber-enabled information operations); *attacking trust in military information or systems* (“undermining the adversaries’ confidence in his capabilities,” a core capability in a 2003 “roadmap” signed by the U.S. secretary of defense)⁹; and *attempting to defeat physical infrastructure* (such as the electrical grid) *or weapons systems* (such as integrated air defenses).

Other research has included some of these distinctions — especially between exploitation and disruption — but have not also included attacks on trust or compared when and where offensive cyber operations occur on the battlefield.

These are fuzzy categories with substantial overlap. The intent that motivates an offensive cyber operation is often not obvious. Moreover, warfare is messy and resists easy characterization. Accordingly, these categories are best used as loose guides.

That said, an important distinction of the framework presented here — and one made many times by Moore and others — is between the exploitation of information and disruption (computer network exploitation and computer network attack, in military terms). The framework goes further, making the rarer distinction between an operation that is intended to attack the information or system itself and an operation that is attacking the *trust* that the other side places in the information or system. Many offensive cyber operations could be intended to do both, with erosion of trust being an acceptable outcome if a hard kill proves too difficult. The category “defeat physical infrastructure or weapons system” is meant to capture an operation that is intended to directly take a physical object out of the fight, rather than just, say, launch a denial-of-service attack on a military network, another tricky distinction.

Other research has included some of these distinctions — especially between exploitation and disruption — but have not also included attacks on trust or compared when and where offensive cyber operations

5 *The Economist*, “Lessons from Russia’s Cyber-war in Ukraine.”

6 The main effort to categorize such operations (which led to the publication of “Evaluating Assumptions About the Role of Cyberspace in Warfighting: Evidence from Ukraine,” by Erica Lonergan, Margaret Smith, and Grace Mueller, 2023) was inspired by this framework and the research done in partnership with Columbia University.

7 My thanks to Dr. Erica Lonergan for raising this point.

8 Daniel Moore, *Offensive Cyber Operations: Understanding Intangible Warfare* (Oxford: Oxford University Press, 2022), VII.

9 *Information Operations Roadmap, October 30, 2003, Secret [Excised]*, U.S. Department of Defense, available at National Security Archive, <https://nsarchive.gwu.edu/document/16822-department-defense-information-operations>.

| | Exploit Information <i>(Presence-Based)</i> | Attack Information, Networks, and IT Systems <i>(Event-Based)</i> | Attack Trust in Institutions or Erode Morale <i>(Event-Based)</i> | Attack Trust in Military Information or Systems <i>(Presence- or Event-Based)</i> | Defeat Physical Infrastructure or Weapons Systems <i>(Event-Based)</i> |
|--|---|--|---|---|---|
| Before Hostilities <i>(Phases 0 and 1)</i> | Extensive Russian espionage and preparation of battlefield in Ukraine (2022) | Russian “WhisperGate” attack on Ukrainian infrastructure and government (2022) | Russian defacement of Ukrainian government webpages with false messages (2022) | No exact examples found of attacking trust as primary goal of offensive cyber operation As potential secondary goal or additional impact: U.S.-Israeli “Stuxnet” operation against Iranian nuclear enrichment (20??–2012) Chinese theft of blueprints for Joint Strike Fighter (2007) | Russian “Black Energy” and “Industroyer” disruptions of Ukrainian power grid (2015 and 2016) |
| During Hostilities: Before Battle or in the Rear Echelon <i>(Phases 2 and 3)</i> | Russian “Gamaredon” espionage campaign to support invading forces (2022–2023) | Russian disruption of Ukrainian telecommunications (2022) | Russian military intelligence telegraphing disruptive offensive cyber operations for second-order psychological impact (2023) | Attempt of Russian-aligned hackers to erode trust in Ukrainian “Delta” battle-management system (2022) | Russian “AcidRain” disruption of Viasat satellite terminals used by Ukraine and others (2022) |
| During Hostilities: Battle | Possible Russian implant to track Ukrainian howitzers (2016) | Israeli “Operation Orchard” against Syrian air defense (2008) | Possible Russian cyber-enabled information operations to erode Ukrainian battlefield morale (2022–present) | No exact examples found | Russian and Ukrainian hacking of battlefield drones (2022–present) |

Table 1: Framework of Offensive Cyber Operations in Wartime

occur on the battlefield.¹⁰ The one example that explicitly includes the phases of a conflict was inspired by earlier work on the Framework for Offensive Cyber Operations in Warfare.¹¹ Other important research, such as that conducted by Joshua Rovner, discussed similar factors but without providing a formal framework.¹² Accordingly, the Framework for Offensive Cyber Operations in Warfare should substantially improve analytical methodologies and outcomes.

The Timing and Intent of Offensive Cyber Operations

Providing a transparent analytical model, backed with examples from history, will better enable assessments of the impact of offensive cyber operations

in wartime. The framework presented here distinguishes between the when and where of a cyber operation — before hostilities, before the battle or in the rear echelon, or during the battle (that is, in a head-to-head tactical engagement between forces) — and the intended effect of the operation: to exploit information or to disrupt information, networks, systems, trust, critical infrastructure, or weapons systems. This section presents examples of offensive cyber operations that took place in these different phases and that had varying intents.

Before Hostilities

Operations that take place before hostilities are not wartime operations per se, but they create the conditions of success in armed conflict sometime in the future or in the “strategic competitive space”

10 See, for example, Brandon Valeriano and Ryan C. Maness, “The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11,” *Journal of Peace Research* 51, no. 3 (May 2014): 347–60, <https://doi.org/10.1177/0022343313518940>.

11 See Erica D. Lonergan, Margaret W. Smith, and Grace B. Mueller, “Evaluating Assumptions About the Role of Cyberspace in Warfighting: Evidence from Ukraine,” in *15th International Conference on Cyber Conflict: Meeting Reality*, ed. T. Jancarkova, et al. (CCDCOE Publications, 2023), https://www.ccdcoe.org/uploads/doc/CyCon_2023_book_print.pdf.

12 Rovner, “Cyberspace and Warfighting.”



below the threshold of armed conflict.¹³ In Defense Department doctrine, this includes operations that take place in Phases Zero or One: shaping or deterring.¹⁴ States often use offensive cyber operations during these phases as a substitute for other kinds of power, “to degrade or destroy enemy capabilities in peacetime, rather than being forced to initiate and engage in costly conflicts in the physical world.”¹⁵

Such offensive cyber operations that take place before hostilities might include tactics like those used in the U.S.-Israeli Stuxnet operation against Iran’s nuclear enrichment program.

Tactics to exploit information include gaining exquisite military intelligence to learn of strategic or military plans or for operational preparation of the environment. In the run-up to Russia’s 2022 invasion of Ukraine, Microsoft detected Russian “efforts to gain initial access to targets that could be used to provide both intelligence on Ukraine’s military and foreign partnerships,” and “access to critical infrastructure for future destruction.”¹⁶ Such intrusions constitute normal intelligence preparation of the battlespace and are common for most advanced militaries. In a 2008 operation called Buckshot Yankee,¹⁷ “extensive penetration of U.S. government networks had presumably provided Russian intelligence services with aggressive visibility into current deployments, future planning, and policymaker thinking,” access which might be decisive in armed conflict.¹⁸

Another way to exploit information is by stealing technological advantages that are useful to the battlefield. One example is China’s cyber theft of the blueprints for the Joint Strike Fighter and its deployment of a copy.¹⁹

One month before Russia invaded Ukraine, it launched attacks in two additional categories of the Framework of Offensive Cyber Operations in wartime: attacking information, networks, and IT systems as well as undermining trust in institutions or eroding morale. Microsoft has reported that the day before the 2022 invasion, “operators associated with the GRU, Russia’s military intelligence service, launched destructive wiper attacks on hundreds of systems in Ukrainian government, IT, energy, and financial organizations.”²⁰ To undermine trust before the invasion, “Ukrainian government websites, including that of the Ministry of Foreign Affairs, were defaced with a message in Russian, Ukrainian, and Polish claiming that data had been deleted from government servers and would be released.”²¹

Tactics that fall under these two categories might also shape the strategic environment for victory without fighting. Some claim, for example, that China’s leadership is following the precepts of Sun Tzu to use cyber tools to win without war, since “supreme excellence consists in breaking the enemy’s resistance without fighting.”²² Russia has interfered in elections in the United States,²³ Ukraine,²⁴ and elsewhere²⁵ in order to disrupt morale and undermine governments. In the language of persistent engagement, such cy-

13 Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford: Oxford University Press, 2022).

14 *Joint Publication 3-0, Joint Operations*, The Joint Chiefs of Staff, Oct. 22, 2018), v-13, https://irp.fas.org/doddir/dod/jp3_0.pdf.

15 Nadiya Kostyuk and Erik Gartzke, “Why Cyber Dogs Have Yet to Bark Loudly in Russia’s Invasion of Ukraine,” *Texas National Security Review* 5, no. 3 (Summer 2022): 113–26, <http://dx.doi.org/10.26153/tsw/42073>.

16 “Special Report: Ukraine, An Overview of Russia’s Cyberattack Activity in Ukraine,” Microsoft, Digital Security Unit, April 27, 2022, 4, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd>.

17 Ellen Nakashima, “Cyber-intruder Sparks Response, Debate,” *Washington Post*, Dec. 8, 2011, https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

18 J. D. Work, “Burned and Blinded: Escalation Risks of Intelligence Loss from Countercyber Operations in Crisis,” *International Journal of Intelligence and Counterintelligence* 35, no. 4 (2022): 806–33, <https://doi.org/10.1080/08850607.2022.2081904>.

19 Siobhan Gorman, August Cole, and Yochi Dreazen, “Computer Spies Breach Fighter-Jet Project,” *Wall Street Journal*, April 21, 2009, <https://www.wsj.com/articles/SB124027491029837401>.

20 Microsoft, “Special Report: Ukraine, An Overview of Russia’s Cyberattack Activity in Ukraine.”

21 Alden Wahlstrom, et al., “The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine,” Mandiant Blog, May 19, 2022, <https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine>.

22 Kenneth Geers, “Sun Tzu and Cyber War,” Cooperative Cyber Defense Centre of Excellence, Feb. 9, 2011, <https://media.defcon.org/DEF%20CON%2020/DEF%20CON%2020%20presentations/DEF%20CON%2020%20-%20Kenneth-Geers-Sun-Tzu-and-Cyber-War.pdf>.

23 “Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views,” Select Committee on Intelligence, U.S. Senate, Report 116-XX, 116th Congress, 1st Session, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

24 “Foreign Interference in Ukraine’s election,” Atlantic Council, May 15, 2019, <https://www.atlanticcouncil.org/in-depth-research-reports/report/foreign-interference-in-ukraine-s-election/>.

25 Maggie Tennis, “Russia Ramps Up Global Elections Interference: Lessons for the United States,” Center for Strategic and International Studies, July 20, 2020, <https://www.csis.org/blogs/technology-policy-blog/russia-ramps-global-elections-interference-lessons-united-states>.

ber operations “short of armed conflict can have a cumulative impact on the strategic level [and] can damage or degrade ... sources of national power.”²⁶

An adversary might use cyber capabilities to disrupt the flow of logistics into a military theater (an attack on information, networks, and IT systems), perhaps to delay a force’s arrival until after the decisive moment. This is a longstanding Department of Defense concern given that “over 90 percent of [Defense Department] deployment and distribution transactions are handled on unclassified systems.”²⁷ In 1991, the department feared a massive logistics disruption as Dutch hackers “modified or copied unclassified but sensitive information related to U.S. war operations”²⁸ during the run-up to the first Gulf War.²⁹ In what turned out to be a coincidence, the Defense Department feared that the Solar Sunrise campaign of February 1998 was intended to disrupt Operation Desert Fox, a show of force against Iraq.³⁰

The goal of an attack against trust in military information or systems is to erode confidence that a technological or operational system works as intended. Such offensive cyber operations that take place before hostilities might include tactics like those used in the U.S.-Israeli Stuxnet operation against Iran’s nuclear enrichment program. The primary goal appears to have been to destroy war-related infrastructure, but attacking trust was a key component of the operation. David Sanger quoted one participant involved in Stuxnet as saying:

“The intent was that the failures should make them feel they were stupid, which is what happened,” the participant in the attacks said. When a few centrifuges failed, the Iranians would close down whole “stands” that linked 164 machines, looking for signs of sabotage in all of them. “They

overreacted,” one official said. “We soon discovered they fired people.”³¹

Likewise, the abovementioned Chinese theft of blueprints for the Joint Strike Fighter was assumedly intended primarily to gain secret information. But a secondary goal (or incidental impact of the operation) might have been to undermine trust in that platform.

Attacking physical infrastructure and weapons systems includes disrupting militarily relevant infrastructure, such as was the case when Russia disrupted Ukraine’s power grid in both 2015 and 2016.³² It also includes sabotaging militarily relevant capabilities. This could include the “left-of-launch” offensive cyber campaign,³³ in which the United States allegedly sabotaged North Korean ballistic missile launches to slow down development of the overall program.

Offensive cyber operations may also include coercion, but as this topic is covered in great depth by other authors it is not included in this paper, which is primarily focused on the tactical and operational levels of warfare.³⁴

During Hostilities: Before Battle or in the Rear Echelon

Once hostilities have opened, the time for shaping or deterring operations is over. Offensive cyber operations that take place during Phases Two or Three — seizing the initiative or domination, in Defense Department lingo — are no longer used as a substitute for other kinds of power, but as a complement to them or as an independent capability.³⁵ For the U.S. military, such operations are likely to be “pre-allocated to support a specific aspect of an Operations Plan or Contingency Plan” or “allocated to a Combatant Commander.”³⁶ The bulk of the existing examples of offensive cyber operations that occur

26 Michael P. Fischerkeller and Richard J. Harknett, “Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation,” *Cyber Defense Review*, Special Edition: International Conference on Cyber Conflict (2019): 267–87, <https://www.jstor.org/stable/26846132>.

27 “Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors,” U.S. Senate, Committee on Armed Services, 113th Congress, 2nd Session, 2014, https://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf.

28 “Hackers Entered Pentagon Computers,” *Washington Post*, Nov. 21, 1991, <https://www.washingtonpost.com/archive/politics/1991/11/21/hackers-entered-pentagon-computers/b96aad02-d86b-4d69-83cf-b718bf947b54/>.

29 Jack L. Brock, “Computer Security, Hackers Penetrate DOD Computer Systems,” U.S. General Accounting Office, Testimony Before the Subcommittee on Government Information and Regulation, Committee on Governmental Affairs, U.S. Senate, Nov. 20, 1991, <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-006.pdf>.

30 Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace 1986 to 2012* (Washington, D.C.: Cyber Conflict Studies Association, 2013), 120–35.

31 David E. Sanger, “Obama Ordered Speed Up Wave of Cyberattacks Against Iran,” *New York Times*, June 1, 2012, <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>.

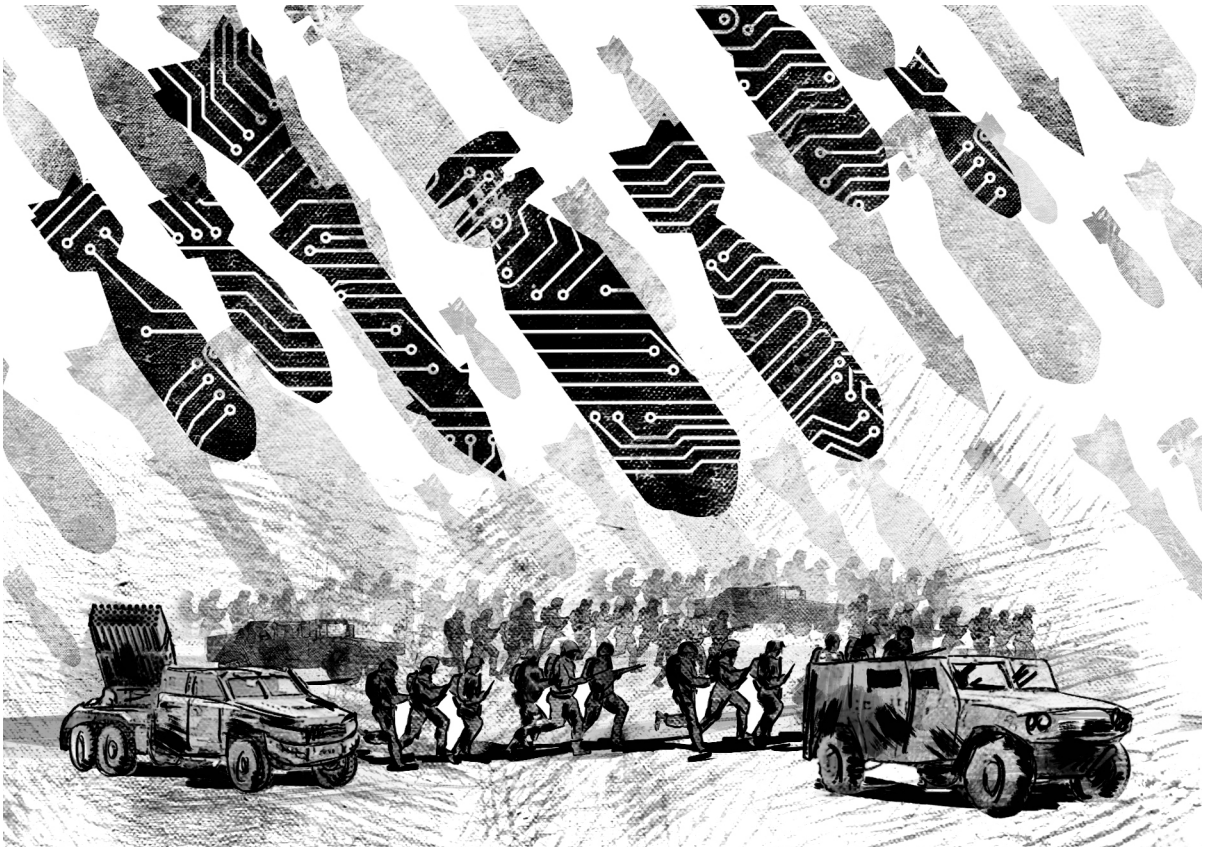
32 Andy Greenberg, “Crash Override: The Malware That Took Down a Power Grid,” *Wired*, June 12, 2017, <https://www.wired.com/story/crash-override-malware/>. Note: This attack did happen during an armed conflict between Ukraine and Russia but is included here as “before hostilities” because the fighting, while intense and bloody, was relatively localized compared to the full-scale invasion of February 2022.

33 William J. Broad and David E. Sanger, “U.S. Strategy to Hobble North Korea Was Hidden in Plain Sight,” *New York Times*, March 4, 2017, <https://www.nytimes.com/2017/03/04/world/asia/left-of-launch-missile-defense.html>.

34 For example, see Erica Lonergan and Michael Poznansky, “Are We Asking Too Much of Cyber?” *War on the Rocks*, May 2, 2023, <https://warontherocks.com/2023/05/are-we-asking-too-much-of-cyber/>.

35 Kostyuk and Gartzke, “Why Cyber Dogs Have Yet to Bark Loudly in Russia’s Invasion of Ukraine.”

36 Department of Defense, *Information Operations Roadmap*, 57.



during hostilities appear to fall into this category, rather than taking place on the battlefield itself.

Offensive cyber operations that are conducted during hostilities more often have a disruptive component, meaning they are typically event-based. Moore noted the key reasons for this:

Like firing a weapon, an event-based operation entails sending a payload from attacker to target in the hope of immediately reducing its integrity or capacity to operate. As a result, these capabilities are often more tactical in nature, easier to integrate with existing military OODA [observe-orient-decide-act] loops and are promising candidates for joint warfare.³⁷

Russia's use of offensive cyber operations has followed this model. The country has "overwhelmingly opted to deploy ... 'pure' disruptive tools," according to Mandiant, a leading cyber intelligence and cyber response company.³⁸ These "pure" disruptive tools

are "lightweight in design and primed for immediate use, containing only the capabilities required to disrupt or deny access to the target system."

Techniques to exploit information could include stealing an adversary's battleplan or trying to understand the location of its tactical assets. Russia's Gamaredon group, associated with the Russian Federal Security Service (FSB), has had a long-running "campaign focused on acquiring military and security intelligence to support potential invading forces."³⁹ Russian intelligence has also spied on Ukraine's rail networks, which are "key to solid and fast heavy weapon delivery to the bases near the frontline." Ukraine has stated that this was done to help Moscow understand "supply dependencies, schedules, and specific equipment/machinery."⁴⁰

Tactics to attack information include disrupting systems that are crucial to mounting an effective defense or disrupting logistics. Since its invasion began, Russia has conducted dozens of attacks to disrupt Ukrainian systems, such as a large-scale

37 Moore, "Offensive Cyber Operations," 96.

38 Dan Black and Gabby Roncone, "The GRU's Disruptive Playbook," Mandiant, July 12, 2023, <https://www.mandiant.com/resources/blog/gru-disruptive-playbook>.

39 Alessandro Mascellino, "Russia-affiliated Shuckworm Intensifies Cyber-Attacks on Ukraine," Infosecurity Magazine, June 16, 2023, <https://www.infosecurity-magazine.com/news/shuckworm-intensifies-ukraine/>.

40 "Russia Cyber Tactics: Lessons Learned 2022," State Service of Special Communications and Information Protection of Ukraine, March 3, 2023, 18, <https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine>.

offensive cyber operation against Ukrtelecom, the main fixed-line telecommunications company, in March 2023.⁴¹

While these operations have not had a lasting or strategic impact, Russia has had more success with this technique in the past by disrupting communications. During Russia's 2008 invasion of Georgia, "computer researchers had watched as botnets were 'staged' in preparation for the attack, and then activated shortly before Russian air strikes," which started the war.⁴² According to a review on the 20th anniversary of the attack, "thirty-five percent of Georgia's Internet networks suffered decreased functionality during the attacks, with the highest levels of online activity coinciding with the Russian invasion of South Ossetia. ... Even the National Bank of Georgia had to suspend all electronic services" for 11 days due to the cyber disruption.⁴³ More recently, in Operation Glowing Symphony in 2015 and 2016, U.S. Cyber Command unleashed substantial power to disrupt the Islamic State's social media and internet propaganda.⁴⁴

However, as military dependence on information technology grows, there are fewer options for such workarounds. There are, after all, only so many fax machines, sextants, or printed maps to go around.

Techniques to undermine trust in the government or erode public morale include a range of cyber-enabled information operations. One possible way to erode trust and morale was made clear from an accident: If Hawaii can, in error, send a warning about an incoming intercontinental ballistic missile, as it did in 2018, an adversary might do so deliberately during wartime to cause panic.⁴⁵

However, as with most categories in the framework presented here, the war in Ukraine provides the

most concrete examples. Mandiant has found that Russian military intelligence set up fake hactivist identities "to claim responsibility for cyber attacks and leak stolen documents or other proofs from their victims." Their goal was "almost certainly an attempt to prime the information space with narratives of popular support for Russia's war and to generate second-order psychological effects" from the initial offensive cyber operation.⁴⁶

Earlier Russian attacks on Media Group Ukraine that planted false messages that Ukrainian President Volodymyr Zelensky had surrendered were likely not intended to trick Ukrainian defenders to lay down their arms, but rather to "erode confidence in Ukrainian media outlets and institutions."⁴⁷

Offensive cyber operations that take place before battle or in the rear echelon can also be used to erode trust in weapons systems or physical infrastructure. In late 2022, a Russian-affiliated hacker claimed to have gained illicit access to Delta, a Ukrainian battle-management system. He posted screenshots of the locations "of friendly troops, enemy troops, barracks, ammunition depots, intelligence data and other information."⁴⁸ Such operations need not be obvious or even detected to cause a loss of trust: "Subtle malicious manipulation of command and control telemetry, or minute disturbances in targeting latency could wreak havoc across an entire operational theatre."⁴⁹ Offensive cyber operations might cause enough disruption to a system that its operators just learn to ignore it and rely instead on workarounds that might adversely impact their readiness to fight: "The mission planning system is 'fubar' yet again. We gotta switch to pencil and paper for the third time today." However, as military dependence on information technology grows, there are fewer options for such workarounds. There are, after all, only so many fax machines, sextants, or printed maps to go around.

41 Thomas Brewster, "'Most Severe' Cyberattack Since Russian Invasion Crashes Ukraine Internet Provider," *Forbes*, March 28, 2022, <https://www.forbes.com/sites/thomasbrewster/2022/03/28/huge-cyberattack-on-ukrtelecom-biggest-since-russian-invasion-crashes-ukraine-telecom/?sh=2073342a7dc2>.

42 John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, Aug. 12, 2008, <https://www.nytimes.com/2008/08/13/technology/13cyber.html>.

43 Sarah P. White, *Understanding Cyberwarfare: Lessons from the Russia Georgia War*, Modern War Institute, March 20, 2018, <https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/>.

44 "Operation Glowing Symphony J3 AAR Observations," U.S. Cyber Command, Nov. 22, 2016, available at National Security Archive, <https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscycbercom-after-action-assessments-operation-glowing-symphony>.

45 Adam Nagourney, David Sanger, and Johanna Barr, "Hawaii Panics After Alert About Incoming Missile Is Sent in Error," *New York Times*, Jan. 13, 2018, <https://www.nytimes.com/2018/01/13/us/hawaii-missile.html>.

46 Black and Roncone, "The GRU's Disruptive Playbook."

47 Kate Conger, "Hackers' Fake Claims of Ukrainian Surrender Aren't Fooling Anyone. So What's Their Goal?" *New York Times*, April 22, 2022, <https://www.nytimes.com/2022/04/05/us/politics/ukraine-russia-hackers.html>.

48 Jenna McLaughlin, "Inside Russia's Attempts to Hack Ukrainian Military Operations," *NPR*, Aug. 10, 2023, <https://www.npr.org/2023/08/10/1193167328/russia-hack-ukraine-military>.

49 Moore, "Offensive Cyber Operations," 115.



Had Buckshot Yankee, Russia's infiltration of classified Defense Department networks, occurred during actual hostilities with the United States, the American military might have had to abandon the entire network until it was resolved. Even a suspicion that an adversary could read (or modify) battle plans and intelligence could be enough to force a military to use less efficient alternatives. Such an attack could have strategic political effects, if it occurred in the systems of, say, a NATO ally, who might then be ejected or quarantined from allied military command-and-control networks so as not to infect others.

Highlighting the substantial overlap between disrupting a system and disrupting trust in that system, the "left-of-launch" cyber operations that the United States launched to disrupt North Korean missile tests may have also been intended (or had the effect of) eroding that regime's confidence that their missiles would be dependable during wartime.

Attacks against physical infrastructure or weapons systems can be used as an independent capability to strike fixed targets behind the battle lines or interdict military forces moving there. Both before the invasion and after, Russian cyber operators disrupted Ukraine's Viasat commercial satellite communications network,⁵⁰ "taking out major [command-and-control] infrastructure critical to managing the military and the country during wartime."⁵¹ In April 2022, Russian military intelligence was frustrated in its attempt to deploy "Industroyer2 malware against high-voltage electrical substations," which had been programmed weeks before to detonate on April 8, 2022 and disrupt electrical power in Ukraine.⁵²

During Hostilities: Battle

Offensive cyber operations also may play important roles during tactical engagements — whether large-scale battles between corps or fleets or local fights between individual platoons, ships, or aircraft. This generally takes place in Defense Department Phase 3 — dominate — but it also includes any violent military engagement, including raids or border

skirmishes. "Battle" and "battlefield" are accordingly used as a loose description of tactical engagements.

The basics of using cyber capabilities to exploit information, the first subcategory, are broadly similar to using older technologies. For example, a normal target of signals intelligence — such as listening to and decoding Morse code over high-frequency transmissions, a mission of my first unit in military intelligence — are appropriate for cyber capabilities as well. In an exercise in the mid-1990s, the first combined offense-defense cyber unit stole the blue-force's Air Tasking Order within two hours,⁵³ giving them perfect knowledge of the next day's raids. A Ukrainian commander has claimed that his unit hacked a Russian drone's video feed to determine its home base, which was then shelled.⁵⁴

Such use of offensive cyber operations could be used to monitor an adversary's common operating picture in real time (which might be accomplished using traditional signals intelligence) or track and follow *every one* of a certain type of unit or platform (which would be very difficult). For example, according to reporting by CrowdStrike, in 2016, Russian military intelligence knew the exact location of Ukrainian D-30 howitzers, having implanted malware in the Android software used by 9,000 artillery soldiers to coordinate their fires.⁵⁵

As modern armies kit their soldiers out with smart or radio frequency identification-equipped rifles and wearable computers for situational awareness (such as the U.S. Army's Nett Warrior for Rangers and other elite troops, based on a Samsung Galaxy Note II phone), it might be possible for a future adversary to know the exact location of every individual soldier or weapons system on the battlefield.⁵⁶

The next subcategory is attacks against information, networks, and IT systems. Disrupting information using cyber capabilities is one obvious tactic. In the 1980s, the United States appears to have discovered a critical vulnerability "in the Soviet Union's high-frequency command-and-control communications that could be exploited to shut down ... orders

50 Anthony J. Blinken, "Attribution of Russia's Malicious Cyber Activity Against Ukraine," U.S. Department of State, May 10, 2022, <https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/>.

51 The Grugq, "Foghorn: Signals Through the Fog of War," grugq substack, June 1, 2022, <https://grugq.substack.com/p/foghorn-signals-through-the-fog-of?s=r>.

52 "Industroyer2: Industroyer reloaded," We Live Security, ESET, April 12, 2022, <https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/>.

53 "Transcript: Lessons from Our Cyber Past – The First Military Cyber Units," Atlantic Council, March 5, 2012, <https://www.atlanticcouncil.org/commentary/transcript/transcript-lessons-from-our-cyber-past-the-first-military-cyber-units/>.

54 David Axe, "Ukrainian Marines Hacked a Russian Drone to Locate Its Base—Then Blew Up the Base with Artillery," *Forbes*, Nov. 30, 2023, <https://www.forbes.com/sites/davidaxe/2023/11/30/ukrainian-marines-hacked-a-russian-drone-to-locate-its-base-then-blew-up-the-base-with-artillery/?sh=29777e262068>.

55 Adam Meyers, "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units," CrowdStrike, Dec. 22, 2016, <https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/>.

56 James Laporta, Justin Pritchard, and Kristin M. Hall, "Military Units Track Guns Using Tech that Could Aid Foes," *AP*, Sept. 30, 2021, <https://apnews.com/article/rfid-military-weapons-guns-62c88008478f4ac403047c21f3184677>; and Sydney Freedberg Jr, "Army Patches Its Network for Near Term," *Breaking Defense*, March 20, 2018, <https://breakingdefense.com/2018/03/army-patches-its-network-for-near-term/>.

from the high command to its strategic missile forces, submarine fleet, and air forces.”⁵⁷

Cyber capabilities might also be used to modify information, the next subcategory, during a tactical engagement. During Operation Orchard in 2008, the Israeli air force apparently used a secret cyber capability called Senior Suter.⁵⁸ Jamming Syrian air-defense radars would have left telltale signs, tipping off operators that something was amiss, so Senior Suter apparently showed operators a blank screen, instructing the computer not to display the incoming Israeli strike aircraft. More insidiously, an adversary could manipulate Air Tasking Orders or the common operating picture, even representing hostiles as friendlies or vice versa. Such an operation would be highly likely to erode operator trust in those systems, which might be an additional goal of the campaign.

Modifying information might affect theater-wide command and control. Russia’s access to U.S. classified systems during the abovementioned Buckshot Yankee operation in 2008 demonstrates the possibilities: Plans and orders might not just have been deleted but changed. Even if it may seem implausible that such an operation could be launched successfully against hardened U.S. classified networks, Iranian networks might not be so robust against U.S. Cyber Command or Israel’s Unit 8200. Nor might India and Pakistan, or Azerbaijan and Armenia have networks that are strong enough to resist attack from the other.

Offensive cyber operations are far more novel when it comes to their ability not just to disable or disrupt but to disrupt all targets with similar characteristics.

Russia’s invasion of Ukraine indicates that militaries might be specifically attacking trust during battle, the fourth subcategory. Russian cyber-enabled information operations have targeted Ukrainian frontline troops with messages like “Your battalion commander has retreated. Take care of yourself.” and “You are encircled. Surrender. This is your last

chance.” These imply that the messages were sent at or near the time of battle.⁵⁹

The fifth subcategory is attack on trust in military information or systems during battle. While the research for this paper found no strong examples, the Russia-aligned hacker who gained access to the Ukrainian Delta battle-management system bragged about having more access than it seems he had actually gained. This was possibly a failed attempt to reduce trust in the system and force Ukraine to use a backup system. According to the U.S. company Recorded Future,

For Delta, trust is crucial. The system enables rapid battlefield communications, ultimately facilitating quicker decision-making. Creating doubt among Ukrainian commanders to make them hesitant to use or share information to the system would have serious repercussions on the war’s outcome.⁶⁰

Techniques to attack infrastructure or weapons systems, the next subcategory, include disabling or disrupting physical infrastructure and weapons systems. While such cases seem to be rare, the Department of Defense had an early scare. In 1998, the guided-missile cruiser USS Yorktown was entirely fitted out with Windows NT, which “reduced the Yorktown crew by 10 percent and saved more than \$2.8 million.” Unfortunately, after a divide-by-zero error in a database manager, the ship was left dead in the water,⁶¹ successfully though ironically reducing sailors’ workload. It is not a stretch to imagine something similar occurring due to enemy action.

While one assessment found “there are no publicly known cases of Russian cyber actors disrupting military equipment in the field,” it does appear that Russian and Ukrainian militaries have been disabling each other’s drones, not with straightforward jamming, but through offensive cyber operations.⁶² One Ukrainian officer claimed that “Ukraine often inserts malicious code into Russian

57 Benjamin B. Fischer, “CANOPY WING: The U.S. War Plan that Gave the East Germans Goose Bumps,” *International Journal of Intelligence and Counter Intelligence* 27, no. 3 (September 2014): 431–64, <https://doi.org/10.1080/08850607.2014.900290>.

58 “The Israeli ‘E-tack’ on Syria – Part I,” *Air Force Technology*, March 9, 2008, <https://www.airforce-technology.com/features/feature1625/>; David A. Fulghum and Douglas Barrie, “Israel Shows Electronic Prowess,” *Aviation Week*, Nov. 26, 2007, <https://aviationweek.com/israel-shows-electronic-prowess>; “Israel Used Electronic Attack in Air Strike Against Syrian Mystery Target,” *ABC News*, Oct. 8, 2007, <https://abcnews.go.com/Technology/story?id=3702807&page=1>.

59 Aaron F. Brantly, Nerea M. Cal, and Devlin P. Winkelstein, *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW*, Army Cyber Institute at West Point, 2017, 36, <https://apps.dtic.mil/sti/pdfs/AD1046052.pdf>.

60 “Joker DPR and the Information War,” Recorded Future, Insikt Group, April 6, 2023, <https://www.recordedfuture.com/joker-dpr-and-the-information-war>.

61 Gregory Slabodkin, “Software Glitches Leave Navy Smart Ship Dead in the Water,” *GCN*, July 13, 1998, available at <https://www.route-fifty.com/digital-government/1998/07/software-glitches-leave-navy-smart-ship-dead-in-the-water/290995/>.

62 Jon Bateman, *Russia’s Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*, Carnegie Endowment for International Peace, December 2022, <https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657>.

drones mid-flight.”⁶³ Ukraine’s defense intelligence has officially claimed to have conducted a “successful attack” against software used by Russian operators to control their drones, leading to a sustained outage.⁶⁴

Such drone hacking is still quite narrow and tactical compared to Nitro Zeus, a large-scale U.S. Defense Department cyber contingency plan, circa 2010, “to disable Iran’s air defenses, communications systems and crucial parts of its power grid.”⁶⁵

Around the same time, the United States considered, but ultimately decided against, using cyber capabilities to “cripple Libya’s air defense and lower the risk to pilots,”⁶⁶ as part of the initial air assault to replace the regime of Muammar Gaddafi. Different policymakers gave competing rationales for not pulling the trigger, such as that the Defense Department wasn’t prepared (“we just ran out of time”⁶⁷) or that, because the United States was punching down, it need not use its most advanced cyber weapons (“these cyber capabilities are still like the Ferrari that you keep in the garage and only take out for the big race and not just for a run around town, unless nothing else can get you there”⁶⁸).

Offensive cyber operations are far more novel when it comes to their ability not just to disable or disrupt but to disrupt all targets with similar characteristics. This is not merely theoretical: Repeatedly in the past, entire organizations, sectors, and nations were knocked offline due to early attacks exploiting common-mode failures, like the Morris Worm (1988) and SQLSlammer (2003). Until just a few months before it struck in 2017, literally every computer running Microsoft Windows was open to the vulnerability behind NotPetya (except, perhaps, those at the National Security Agency, where it was developed). The same is true of weapons systems and sensors. Some future attack might not just take down one guided missile cruiser but every other ship of Ievery type that shared the same vulnerability — and at the same moment.

Moore gives the chilling example of the Tomahawk Strike Network, “which reportedly allows anybody who has the authority

to logon ... [and] take control of the missile,” or indeed all missiles, just as Roger Schell warned in 1979:

*Indeed, if Chinese network forces successfully compromise a TSN control node—a tall order but not impossible—they can effectively neutralize Tomahawks en-route to strike [People’s Liberation Army] missile bases and limit US ability to intervene in the conflict prior to the US Navy’s arrival on the scene. Even if US operators are eventually alerted to a compromise, they will nonetheless be compelled to bring the TSN down pending a forensic investigation in order to avoid possible friendly fire incidents or any further mishandling of launched Tomahawks. For the duration of the conflict, the damage to combat readiness and efficacy would have already been done. Trust in the platform would be impaired, which is possibly an even more damaging prospect than any concrete threat to the missiles themselves.*⁶⁹

What started as an attack against the weapon system itself magnifies in its impact by becoming an attack on trust.

Lastly, offensive cyber operations are not just useful for disrupting infrastructure or a weapon system but for commandeering a target or indeed commandeering all targets with similar characteristics. After all, hacking is all about subverting a computer so that it follows the attacker’s instructions and not the original owner’s.⁷⁰

Not long after Russia’s February 2022 invasion, Google expanded its protection against denial-of-service attacks, allowing Google to absorb the bad traffic in a distributed denial-of-service attack and act as a “shield” for smaller websites in Ukraine.

63 “The Latest in the Battle of Jamming with Electronic Beams,” *The Economist*, July 3, 2023, <https://www.economist.com/special-report/2023/07/03/the-latest-in-the-battle-of-jamming-with-electronic-beams>.

64 “Rashists Suffer — a Large-Scale Failure of Drone Control Software: Details of the DIU Cyberattack,” Ministry of Defense of Ukraine, Defense Intelligence, Feb. 8, 2023, <https://gur.gov.ua/en/content/u-rashystiv-masshtabnyi-zbii-prohramy-keruvannia-dronamy-detali-kiberataky-hur.html>.

65 David Sanger and Mark Mazzetti, “U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict,” *New York Times*, Feb. 16, 2016, <https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html>.

66 Ellen Nakashima, “U.S. Cyberweapons Had Been Considered to Disrupt Gaddafi’s Air Defenses,” *Washington Post*, Oct. 17, 2011, https://www.washingtonpost.com/world/national-security/us-cyber-weapons-had-been-considered-to-disrupt-gaddafis-air-defenses/2011/10/17/gIQAET-pssL_story.html.

67 Nakashima, “U.S. Cyberweapons Had Been Considered.”

68 Nakashima, “U.S. Cyberweapons Had Been Considered.”

69 Moore, “Offensive Cyber Operations,” 196–97.

70 Lennart Maschmeyer, “The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations,” *International Security* 46, no. 2 (Fall 2021): 51–90, https://doi.org/10.1162/isec_a_00418.

As is hopefully clear from this section, analyses of the impact of offensive cyber operations in warfare will be much more effective using frameworks such as the novel one presented here. Analysts need such tools to distinguish the when, where, and what of offensive cyber operations to drive further and better analyses.

Further Research

The framework presented here might itself be further improved with tighter categories for easier coding of large data sets and could be extended with additional examples. As mentioned earlier, it might benefit by including operations that take place outside the conflict zone that are meant to influence the conflict (such as, say, Russian attacks against European energy infrastructure).

The Framework for Offensive Cyber Operations in Warfare could also be substantially improved by incorporating not just *offensive* cyber operations, but *defensive* ones as well.⁷¹ The principal difficulty of including defensive operations is that defense tends to be diffuse, loosely coordinated, and steady state. Offense is conducted by specialized units and is purposeful, is driven by specific objectives, and is time bound. A framework optimized to examine offense, like the framework in this paper, might never be able to adequately address defense. For example, even though much of offensive cyber operations is about attacking trust, it is hard to conceptualize a defensive trust operation for infrastructure or military equipment.

However, this framework can incorporate some aspects of defensive operations, most clearly in what the U.S. Cybersecurity Framework calls the defensive phases of respond — containing the impact from a cyber incident — and recover — resilience to return “to normal operations to reduce the impact from a cybersecurity incident.”⁷² These phases only occur in direct response to a cyber incident and so are similarly purposeful and time-bound. When actions are taken knowing an attack is likely to come, sometimes the protect phase is important as well. Here are some examples of how the framework presented here could be used to categorize defensive cyber operations:

- *Before Hostilities: Defeat Physical Infrastructure or Weapons System.* Ukraine’s power-grid operators and engineers successfully scrambled to limit the damage from the disruptions Russia caused using Industroyer and Black-Energy.⁷³ (Respond phase)
- *Before Hostilities: Attack Information, Networks, and IT Systems.* Microsoft specifically developed and deployed new ways to protect against and better detect Russia’s Whisper-Gate malware, which had been used against Ukraine’s infrastructure and its government.⁷⁴ (Initially the respond phase for Microsoft but feeds other phases for Ukrainian defenders.)
- *During Hostilities, Before Battle or in the Rear Echelon: Defeat Physical Infrastructure or Weapons System.* After Russia’s AcidRain disruption of Viasat terminals, Ukrainian commanders and forces switched to other means of communications to remain resilient.⁷⁵ (Recover phase)
- *During Hostilities, Before Battle or in the Rear Echelon: Attack Trust in Institutions or Erode Morale.* Ukrainian officials claimed, in March 2022, to have disrupted five Russian botnets that had been spreading disinformation. (Respond phase)
- *During Hostilities, Before Battle or in the Rear Echelon: Attack Information, Networks, and IT Systems.* Not long after Russia’s February 2022 invasion, Google expanded its protection against denial-of-service attacks, allowing Google to absorb the bad traffic in a distributed denial-of-service attack and act as a “shield” for smaller websites in Ukraine.⁷⁶ (Protect phase)

Can Cyber Deliver?

The impact of offensive cyber operations in modern warfare in the short term will depend much on the specifics of the capability and the conflict. In the long term, innovations in technology and the frequency and intensity of conflict will likely matter more.

71 Thank you to an anonymous reviewer for this suggestion.

72 *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, U.S. National Institute of Standards and Technology, April 16, 2018, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

73 Andy Greenberg, “How an Entire Nation Became Russia’s Test Lab for Cyberwar,” *Wired*, June 20, 2017, <https://www.wired.com/story/russian-hackers-attack-ukraine/>.

74 “Destructive Malware Targeting Ukrainian Organizations,” Microsoft Security, Jan. 15, 2022, <https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>.

75 Bateman, *Russia’s Wartime Cyber Operations in Ukraine*.

76 Kent Walker, “Helping Ukraine,” Google Article, March 4, 2022, <https://blog.google/inside-google/company-announcements/helping-ukraine/>.



Over the Short Term

Based on the most extensive unclassified modeling of how offensive cyber operations would affect battle outcomes — in this case between U.S. and Chinese fleets — a 2022 paper by J. D. Work found that the success of offensive cyber operations was closely tied to the nature of modern naval warfare. Because large-scale missile exchanges led to a “disproportionate impact of even relatively small advantages,” Work concluded that offensive cyber operations provided substantial “advantage over the adversary, with greater numbers of adversary vessels damaged or sunk where [offensive cyber operations] options were employed in support of missile fires.”⁷⁷

The most impactful offensive cyber operation in wartime will generally be the most difficult, requiring substantial intelligence, patient planning, and advanced capabilities guided by elite operators and open-minded commanders. It will also be limited by extremely high levels of uncertainty. That is, some operations might be astoundingly effective, while others that are seemingly identical may fail entirely. It is difficult to know beforehand which will be which.

It appears, for example, that Russian cyber operations against Ukraine were less than fully effective in part because of a successful defense by Ukraine, which was backed by the global technology sector, volunteers, and U.S. Cyber Command.⁷⁸ So, successful defense is possible, but it is not inevitable. In Ukraine, those defenses have so far prevented any cyber catastrophes, but will they next time? Would Iran’s defense have prevailed against Nitro Zeus or Taiwan’s against the People’s Liberation Army? There is no way to know beforehand.

The rule of thumb in ground warfare is that an attacker should have between a three to one and a six to one advantage to be confident of victory. There can be no such easy estimate in cyber conflict. A global cyber onslaught might be undone by a serendipitous discovery,⁷⁹ one of the best-defended technology giants could be hacked by teenagers,⁸⁰ or attackers might bypass elite defenses just by first compromising a trusted vendor.⁸¹ Defenders might easily swat away 99 offensive cyber operations only

to have the 100th sweep away all before it. While some cyber operations (like intelligence) have lower uncertainty compared to others, all are less predictable than traditional operations.

This is more than just saying there can be David-beats-Goliath upsets: The complexity of cyber space and cyber operations stymies predictions of which side will prevail.

However, even less sophisticated offensive cyber operations could substantially change battlefield outcomes, especially if exquisite insights are gained by cyber-enabled intelligence operations, making the battlefield far more transparent. Relatively unsophisticated operations might help deliver a *fait accompli* — such as China delaying U.S. forces long enough to achieve limited objectives in Taiwan — or be used as an opening attack to “keep the victim reeling when his plans dictate he should be reacting,” in the words of Richard Betts.⁸²

Russia attempted this with its Viasat attack to disrupt Ukrainian command and control, an attack that was only unsuccessful because of Ukraine’s preparation. Russia was more successful during the invasion of Georgia in 2008. While not decisive, those attacks impeded “the Georgian government’s ability to react, respond, and communicate, [creating] the time and space for Russia to shape the international narrative in the critical early days of the conflict.”⁸³

And the Longer Haul

Beyond the next decade, offensive cyber operations in warfare may be less driven by the particulars of one or a few wars, and more driven by the frequency and intensity of global conflicts and the general direction of technological progress. After all, the future will look substantially different than today. Humanity is still only in the first decades of the information age, which, like the agricultural and industrial ages before it, will encompass decades or even centuries.

Wars drive innovation and improvisation. Since most of cyber conflict has occurred during the relative peace of the post-Cold War decades, theories of cyber conflict have been based in false assumptions like that “territorial conquest continues to become

77 J. D. Work, “Offensive Cyber Operations and Future Littoral Operating Concepts,” *Military Cyber Affairs* 5, no. 1, (2022), <https://digitalcommons.usf.edu/mca/vol5/iss1/3/>.

78 Bateman, *Russia’s Wartime Cyber Operations in Ukraine*.

79 Lily Hay Newman, “How an Accidental ‘Kill Switch’ Slowed Friday’s Massive Ransomware Attack,” *Wired*, May 13, 2017, <https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/>.

80 Lawrence Abrams, “Lapsus\$hackers Leak 37 GB of Microsoft’s Alleged Source Code,” *Bleeping Computer*, March 22, 2022, <https://www.bleepingcomputer.com/news/microsoft/lapsus-hackers-leak-37gb-of-microsofts-alleged-source-code/>.


81 Jason Murdock, “Who Has Been Affected by the Huge SolarWinds Cyberattack so Far?” *Newsweek*, Dec. 18, 2020, <https://www.newsweek.com/solarwinds-orion-software-cyberattack-hack-victims-targets-list-1555840>.

82 Richard K. Betts, *Surprise Attack: Lessons for Defense Planning* (Washington DC: The Brookings Institutions, 1982), 5.

83 White, *Understanding Cyberwarfare*.

somewhat more anachronistic.”⁸⁴ Most of the examples in the framework presented above have come from a single war, the Russian invasion of Ukraine, over the past two years. If conflicts between cyber powers become more frequent, offensive cyber operations will continue to be used in surprising ways.

Offensive cyber operations in warfare may also move in surprising directions based on technological changes. Advances in AI since 2022 make it hard to assess the danger of AI-driven offensive cyber operations or promises of AI-driven defenses, though some efforts have been made to assess whether AI will ultimately favor attack or defense.⁸⁵

More generally, if nations successfully secure their critical infrastructure or weapons systems at scale, adversaries will find it nearly impossible to succeed in launching offensive cyber operations for many of the categories of this framework. More likely, however, societies and armed forces will continue to become increasingly dependent on technologies that are not secure, opening themselves to more, and more intense, offensive cyber operations. 

Jason Healey is a senior research scholar at Columbia University’s School of International and Public Affairs. He was a plankholder of the first joint cyber command in 1998 and the White House’s Office of the National Cyber Director in 2022.

Acknowledgments: The author wishes to acknowledge the participants of a workshop on this topic at Columbia University in 2019; research assistance by Chris Smith, Shawn Gibson, and Brian Palacios Paz; previous work going back decades by many academics, analysts, and academics; and the reviews or input by several colleagues (especially by Steve Biddle, Erica Lonergan, Daniel Moore, Greg Rattray, and J. D. Work) as well as several anonymous reviewers.

Image: Staff Sgt. Renee Seruntine⁸⁶

84 Kostyuk and Gartzke, "Fighting in Cyberspace."

85 Jason Healey, "The Impact of Artificial Intelligence on Cyber Offence and Defence," Australian Strategic Policy Institute, Oct. 18 2023, <https://www.aspistrategist.org.au/the-impact-of-artificial-intelligence-on-cyber-offence-and-defence/>.

86 For the image, see <https://www.dvidshub.net/image/7758912/cyber>.