THE CYBER DEFENSE REVIEW
In press, 8 pages
https://doi.org/10.55682/cdr/ahs0-k0pg

SENIOR LEADER PERSPECTIVE

Is Cyberwar War – and Why Might it Matter?

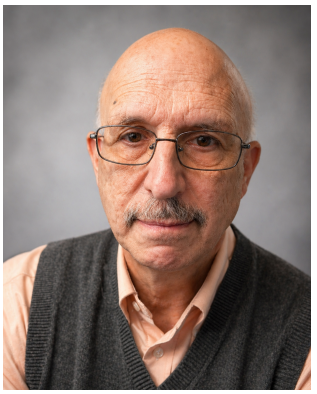
Dr. Martin Libicki*

Former Professor at the U.S. Naval Academy, Annapolis, MD, USA

This article examines the persistent question of whether cyberwar constitutes "war" and why this distinction matters for international stability and escalation dynamics. It argues that attempts to define cyberwar through fixed technical or quantitative criteria—such as scale, damage, or attribution—are ultimately insufficient, as the designation of cyber actions as "war" is inherently political and shaped by strategic interests. The analysis focuses on escalation, particularly the role of thresholds that distinguish escalation by degree from escalation by type, emphasizing how the classification of cyber operations influences whether responses cross into kinetic conflict. The author outlines three perspectives—consensus that cyberwar is war, consensus that it is not, and disagreement between actors—and argues that instability is greatest when perceptions diverge. It further explores the complicating role of cyberespionage, sanctions, and the ambiguous positioning of cyber operations within an "escalation lattice." The article concludes that predictability in how states interpret and respond to cyber operations is essential to reducing miscalculation and unintended conflict, even if clear and universally accepted thresholds remain elusive.

Keywords: cyberwar, escalation, thresholds, use of force, cyberespionage, international stability, conflict dynamics

* Corresponding author: libmazo@gmail.com



Dr. Martin Libicki (Ph.D., U.C. Berkeley 1978) held the Keyser Chair of cybersecurity studies at the U.S. Naval Academy until end-2024. He is the author of a 2016 (2nd edition, 2020) textbook on cyberwar, Cyberspace in Peace and War, as well as three others commercially published books, The New Calculus of Escalation, Conquest in Cyberspace: National Security and Information Warfare, and Information Technology Standards: Quest for the Common Byte. He is also the author of numerous RAND monographs, notably Brandishing Cyberattack Capabilities, Crisis and Escalation in Cyberspace, and Cyberdeterrence and Cyberwar as well as How Insurgencies End (with Ben Connable), and How Terrorist Groups End (with Seth Jones). He is currently developing a video series on conflict escalation. Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years for the GAO.

Whenever there is a sufficiently noteworthy cyber intrusion – be it attack or espionage – policymakers are apt to ask whether it was an act of war. Presumably, their concern is less lexicographical and more one of: do we wish to respond as if it was an act of war? A yes answer can lead to anything from finger-wagging to a response that is similarly warlike (presumably a like-for-like response would not need to ask or answer that question).

Correspondingly, there have been many attempts to delineate characteristics of a cyberattack – e.g., casualty levels, state involvement, the breadth of targets – that would justify such an ascription. That approach seems meaningless. While there are guidelines for judging whether this or that action in the physical world constitutes an act of war (technically, an armed attack or the use of force), extending these into cyberspace by analogy is a fraught exercise. Because the implications of any correspondence between cyberwar and war as we normally understand it are political, any such correspondence must also be political. Hence my response: a cyberattack is an act of war if it is in your interest to deem it so.

Upon (years of) further reflection, it appears that this answer, while not incorrect, is antithetical to stability, as it affords little predictability and may lead to misunderstanding. While there is no *ipso facto* distinction between cyberwar and physical war, there could be some mutual understanding of where a distinction may lie. Absent that, the potential for escalation stemming from the vulnerabilities of cyberspace may be higher than need be.

WHAT IS ESCALATION?

To explain why such a distinction matters requires a dive into the escalation abyss.

What, after all, *is* escalation? The most satisfactory definition comes from a former RAND colleague, Forrest Morgan, who defined it as “an increase in the intensity or scope of conflict that crosses a threshold considered significant by one or more of the participants.” The keyword, for our purposes, is “threshold” – but why? Escalation may be divided into two types: escalation by degree and escalation by type. Escalation by degree is doing more tomorrow of what you were doing today – think of the three-year process of raising U.S. force levels in the Vietnam War. Escalation by type is doing something tomorrow that you had yet to do – think of a Cold War NATO using tactical nuclear weapons to stop a Soviet conventional invasion. If escalation by degree had thresholds, they could only be arbitrary: e.g.,

when US force levels in South Vietnam exceeded 100,000. But escalation by type is far less arbitrary: a kinetic response to a cyberattack would be such an escalation – but *if and only if* the distinction between cyberwar and kinetic war were recognized as a meaningful threshold.

Crossing a meaningful threshold is a big deal insofar as it signals escalation by one side and justifies, hence facilitates, a like response from the other. States may respond to escalation to seek military advantage that they earlier shied from in hopes that the other side would exercise self-restraint. Or they may seek to re-level the playing field, or signal that they would not back down, or seek to thereby inhibit a repeat performance or, worse, further escalation. But such a response is not automatic. States may also not respond due to a lack of resources or the desire to seize or maintain the moral high ground, or to, more broadly, protect their reputation. But as a rule, the odds that the other side does cross a threshold and thereby, itself, escalate are correlated with the fact of the one side's having done so. A response – or more accurately, a reputation for responding – may inhibit escalation by one's foes, but it also sets up a tit-for-tat competition.

SO, *IS* CYBERWAR WAR?

Now return to the main question. If cyberwar is not war, but sits one or more levels below physical war on the escalation ladder, then the transition from cyberwar to kinetic war is an act of escalation that crosses a threshold. A like-for-like response would not cross a threshold unless there were recognized thresholds *within* the cyberspace portion of the conflict spectrum. If cyberwar is war, then a kinetic response to a cyberattack would be an act of escalation and would, correspondingly, open the door to kinetic counter-responses and so on.

Agreement among rivals that cyberwar is a peacetime activity or agreement that it is a wartime activity are both less escalatory than disagreement on whether cyberwar belongs in war or peace. Here is why, expressed through three alternative perspectives.

Assume, first, that cyberattacks that disable (or, worse, destroy) important systems are universally deemed tantamount to war. Potential aggressors believe that engaging in cyberwar will cause others to see it as war, thereby justifying the other side's escalation to the use of force. So thinking, aggressors would hold off unless either they (1) are prepared to go to war anyway, (2) believe their targets are disinclined to wage war even though they believe that the aggressor has, or (3) hope the other side will not characterize or attribute the attack with enough confidence to react. Here, the bar to cyberwar is high. Critical information systems suffer no state-fostered interference. But crises may erupt from accidents, the mis-characterization of cyberespionage as preparations for cyberwar, misattribution, or claims that some cybercrimes (e.g., ransomware attacks on critical infrastructure such as Colonial Pipeline's) are state cyberattacks by proxy.

Assume, second, cyberattacks are not deemed a use of force or an act of war. Others may respond in kind to hostile cyberspace operations, but not violently. Such kinetic peace, though, is won at the cost of putting up with the depredations of cyberwar. Stability holds, but information and other digital systems remain at risk.

Last, assume opinion is split. Some leaders think cyberattacks do not make for war; others do. If aggressors believe the former and their targets believe the latter—and can do something about it—a confrontation between the two can lead to unexpected kinetic conflict. For instance, the aggressor

wages cyberwar because the step up from everyday hostility is small; to them, cyberwar does not justify a response that uses force. The target reacts to cyberwar by using force because they do not see a transition from cyberwar to physical war as a huge step. Neither side has, in its view, crossed a threshold: the aggressor does not believe that its actions constitute war, but the target concludes that war has already started, and the primary question is how best to conduct it. For stability, this is the worst outcome.

Admittedly, the question may not admit of a yes-or-no answer. A particularly destructive cyberattack may be likened to an act of war, whereas lesser attacks would not. As a practical matter, in the (highly) unlikely event that some cyberattack achieves the damage levels of the 9/11 hijackings (thousands killed, hundreds of billions in damage), a forceful U.S. response would not be seen as disproportionate.

It matters whether thresholds are defined in terms of means—which would differentiate cyberwar and kinetic war—or ends (effects). In the latter case, a cyberattack that broke things and harmed people would cross a threshold. But something like the 2017 NotPetya cyberattack, which cost victims collectively $5 to $10 billion but did not physically injure anyone, would not. Since most cyberattacks—particularly distributed denial of service (DDoS) attacks—are mere nuisances, a threshold might be understood as some minimum level of physical damage. But actual effects may be difficult to measure unambiguously. They may look nothing like intended effects because the cyberattack failed (quite common) or, conversely, the malware used ran amok or induced unexpected cascading damage. But that just introduces a more complicated threshold. The more parts to such a threshold, the more difficult would be a consensus on it. An I'll-know-it-when-I-see-it threshold reintroduces all the instability issues that thresholds are meant to address.

We should note that official or even quasi-official guidance on this question is scant. Despite some consensus that there *should* be norms of international behavior to tame the Wild West of cyberspace, if norms mean that countries refrain from operations that are otherwise in their interest, then there are none today, nor are any likely tomorrow. An argument that the threshold between cyberwar and kinetic war has been normalized insofar as no cyberattack has drawn a physical response (with the Israel-Iran dyad a possible exception) has two problems. It does not cover unprecedentedly damaging cyberattacks, and a failure of a state to respond to a class of insult or injury is not the same as a commitment never to respond.

WHAT ABOUT CYBERESPIONAGE?

If cyberwar is war and no threshold separates cyberespionage from cyberattack, what does that say about the stability of a world in which everyone who can does cyberespionage? At first glance, such parallelism may be a *reducto ad absurdum*.

Collecting information is not considered a legitimate *casus bello* under the *jus ad bellum* norms of the law of armed conflict (LOAC) and has rarely led to war in the past. So, cyberespionage—which comprises most hostile state activity in cyberspace—should never lead to worse. But several features suggest against overreliance on that logic.

One, changes in quantity may imply changes in quality. Traditional espionage stole information about or from one or a handful of people. Cyberespionage, though, can steal information about tens of millions—as China's 2015 theft of U.S. Office of Personnel Management (OPM) records files did. South

Korea spent almost a billion dollars to redo its national identity system after it was compromised by North Korea. Botnets could steal information from millions of machines. So, the seriousness level may be much higher.

Two, even after decades of effort in the cyber community to distinguish cyberespionage and cyberattack, the media and public officials conflate the two.

Three, the early stages of both cyberattack and cyberespionage—penetration of the target system and lateral movement within it—are largely the same, not least because cyberattacks (DDOS attacks aside) often must be preceded by reconnaissance in the form of cyberespionage. Thus, detecting an intrusion into critical systems may alarm defenders who infer that a cyberattack is being prepared or even in progress.

Four, active defenses against cyberespionage, notably "persistent engagement," can easily include cyberattacks, undertaken to affect the ability of the other side's hackers to use their own systems (albeit to harm others). The target of these active defenses may easily shrug this off as spy-versus-spy games that imply nothing higher. But leaders inclined to strike back can use these games to argue that they did not go first. And, if one side is unlucky, the target – and it may be unintended – of some active defense may be deemed a sensitive system.

All this suggests that a combination of a rush to judgment, such as a worst-case assessment of cyberespionage, or equilibrating cyberespionage and cyberattack together with deeming cyberwar as tantamount to war in general, can be quite destabilizing. If the latter cannot be avoided, the former should be.

IS CYBERWAR AN ESCALATION VIS-À-VIS SANCTIONS OR THE REVERSE?

Despite the common metaphor of escalation as a ladder – where any state of play is either more or less intense than another – it is often more like a lattice in which it is unclear whether one state is more or less intense than another. This is true, in large part because of domains such as cyberspace where, say, it is not inherently obvious that small kinetic attacks possess more intensity than large cyberattacks or *vice versa*. This leads us to ask whether the favorite U.S. response to cyberspace intrusions – levying sanctions on individuals and even nations – is akin to escalation or de-escalation. If deemed escalation, further escalation by the other side is more likely than otherwise.

Although Russia's economic retaliation for being hit by economic sanctions was relatively weak (as befit its weak economy), Russia could have used cyberattacks to press the West for sanctions relief. Conversely, would that have been escalation? And would it have lubricated a transition between economic "war" and kinetic conflict among nuclear powers?

As of this writing, Russia has not carried out much in the way of consequential cyberattacks on the West—and much of what it did, at least in the first few years, was aimed at hobbling supplies going to Ukraine. Western customers of Russia's February hack of Viasat satellite terminals meant to cut Ukrainian wartime communications were, at most, collateral damage. Maybe because Putin's hackers only had six weeks' notice of the invasion, they had too little time to prepare serious hacks in retaliation for sanctions. Yet by 2024, that rationale lost its explanatory power. Perhaps Russia believes

that cyberattacks on U.S. critical infrastructure could free U.S. CYBERCOM to target Russian military systems.

A Russian cyberattack on Western systems might be understood as escalation vis-à-vis sanctions if escalation is understood as one side doing something that both sides hitherto refrained from doing. Otherwise, the answer may depend on where cyberwar sits on the escalation lattice. Russian officials have called economic sanctions, and especially the cut-off from the SWIFT funds transfer system, acts of economic war, clearly hinting that they stand at the same level as violent warfare. But sanctions are the converse of trade, a set of arrangements freely entered into. Thus, they can be freely exited from as well (subject to contract law and trade agreements). LOAC does not recognize sanctions, even *qua* economic warfare, as the use of force. Correspondingly, being victimized by sanctions cannot justify the use of force. Cyberattacks, conversely, are imposed by attackers on victims; they are nonvoluntary.

From another perspective, economic sanctions can be far more economically damaging than the most expensive cyberattack—NotPetya. Even a 2 percent drop in Russia's GDP from their effects, as happened in 2022 (but not in subsequent years) could cost tens of billions of dollars – well in excess of the $5 to $10 billion, as noted, associated with NotPetya. By such criteria, cyberwar would likely be less costly, hence not an escalation. The West in general may push back on such an equivalence, in part because it enjoys a clear advantage in economic sanctions but has no such obvious advantage in cyberwar. But for just that reason, the West's rivals may favor the opposite.

Again, different perceptions about cyberwar's place in the escalation lattice may grease the transition from economic sanctions to kinetic warfare. One side imposes sanctions on the other side, which suffers large losses and then retaliates with cyberattacks to cause comparable losses to make the one side stop imposing sanctions. The one side, in turn, deems cyberwar to be war. It could retaliate with kinetic attacks. A potential firebreak might differentiate cyberattacks that leave casualties (hence, like war) from those that do not (hence, unlike war). But given the difficulties of predicting the effects of cyberattacks, such a firebreak may be crossed unintentionally.

HOW URGENT IS THIS QUESTION?

Legitimate concerns remain that escalation into war may result from a campaign of cyberattacks (particularly if it included electronic warfare, psychological operations, and coercive surveillance). Yet it is neither certain nor particularly likely that cyberwar can push countries to war if they are otherwise disinclined to do so.

Escalation presumes that cyberwar is successful at the technical level and that success makes it difficult not to respond for political reasons, psychological ones, or to regain some military balance. The unexpected escalation to physical war requires an aggressor who does not see cyberwar as tantamount to violence, and a target who determines that yes, it is—and needs to make a violent response. In principle, the only way cyberattacks should persuade a rational state to escalate to kinetic conflict is if (1) *future* such cyberattacks would be intolerable, (2) there are no other ways to ward off or mitigate such attacks, and (3) the use of force would end such cyberattacks or at least reduce them to a tolerable level without leading to something worse. Meeting each criterion – much less all – is nontrivial.

Increasingly, cyberwar appears to be in the process of being normalized as something distinct from war. The Russian invasion of 2022 was clearly a more intense fight than the gray zone takeover of Crimea and the eastern Donbass—but the level of *successful* cyberspace activity by Russia in both cases was comparable. Persistent engagement—if it entails cyberattacks on other countries' hackers—appears to be an escalation vis-à-vis the cyberespionage activity it is intended to suppress, but reaction to such escalation, so far, has been muted. In what other military domain would an ongoing attempt to degrade the other side's capabilities be normalized?

Could this change? Do cyberattacks occupy a low niche on the escalation spectrum because of their inherent nonviolent and transitory character or because their efficacy, so far, has been unimpressive compared to serious violence? Are cyberwar's consequences so awful that countries are restraining themselves for fear of mutually assured disruption? Or more prosaically, have the results of cyberwar been so restrained, as more system operators take cybersecurity seriously, making national-level consequences harder to achieve?

The place of cyberwar on the escalation lattice remains undecided. In the early months of the Russo-Ukrainian war, commentators saw cyberattacks (on the West) as an act of escalation *up* from death and destruction (against Ukraine). Secretary of Defense Robert Gates placed cyberattacks between heavy conventional warfare and tactical nuclear weapons: "It [the war in Ukraine] could also end in a Russian escalation, perhaps in the form of cyberattacks or even tactical nuclear weapons" (Ignatius 2022).[1] The Atlantic Council's Richard Hooker (2022) listed "employing cyber tools" as the first of Putin's escalation options, ahead of WMD use. Sanger (2022) also placed cyberattacks first, "if Mr. Putin believes that his conventional military forces are being strangled, he will turn to stepped-up cyberattacks on Western infrastructure, chemical weapons or his arsenal of tactical, 'battlefield' nuclear weapons." [2] Kendall-Taylor and Kofman (2022) or Clement (2022) lumped cyberattacks with nuclear weapons as options for a desperate Putin. In the other direction, analysts have mooted cyberattacks as a satisfactory result to Russian nuclear weapons use in Ukraine (Herken, Cohen, and Moore 2022) or even a dissuasive tool beforehand (Bruusgaard 2023). The same inflation of cyberwar appears in a RAND assessment of a hypothetical war with China (Heath, Gunness, and Finazzo 2022; Wertheim 2022) as well as the DoD's assessment (Department of Defense 2023).

CONCLUSIONS

Predictability fosters stability. If each side knew what the other would do in this or that situation, it could tailor its policies accordingly. Its need for worst-case thinking would be abated. And while complete predictability is illusory – war, not least cyberwar, is a chancy endeavor – greater predictability is not.

Exactly how states go about ensuring that the name of the thing – thresholds – matches the nature of the thing – a credible promise not to escalate but to respond if others do – is a different question. States can declare their thresholds, but will others believe them? States can negotiate thresholds with their rivals, but, at least in the case of cyberwar, this requires rivals to admit that cyberwar is not something they would never do (even after building organizations to wage such campaigns). In time,

1. See also The Economist (2022)
2. See also Troianovski and Sanger (2022)

state practice, based on how they react to significant cyberattacks, may set some *de facto* thresholds – but such a process would be long and costly – if the requisite incidents even occur.

REFERENCES

Bruusgaard, Kristin Ven. 2023. "How Russia decides to go nuclear: Deciphering the way Moscow handles its ultimate weapon." *Foreign Affairs* (February 6, 2023). https://www.foreignaffairs.com/ukraine/how-russia-decides-go-nuclear.

Clement, Peter. 2022. "Putin's risk spiral: The logic of escalation in an unraveling war." *Foreign Affairs* (October 26, 2022). https://www.foreignaffairs.com/ukraine/putin-risk-spiral-logic-of-escalation-in-war.

Department of Defense. 2023. *Military and Security Developments Involving the People's Republic of China 2023.* U.S. Department of Defense. https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

Heath, Timothy R., Kristen Gunness, and Tristan Finazzo. 2022. *The Return of Great Power War: Scenarios of Systemic Conflict Between the United States and China.* Santa Monica, CA: RAND Corporation. https://doi.org/10.7249/RRA830-1.

Herken, Greg, Avner Cohen, and George M. Moore. 2022. "3 scenarios for how Putin could actually use nukes." *Politico* (May 16, 2022). https://www.politico.com/news/magazine/2022/05/16/scenarios-putin-nukes-00032505.

Hooker, Richard D. 2022. "Climbing the ladder: How the West can manage escalation in Ukraine and beyond." Atlantic Council, April 21, 2022. https://www.atlanticcouncil.org/in-depth-research-reports/report/managing-escalation-in-ukraine/.

Ignatius, David. 2022. "As Ukraine braces for a second round, the West has a duty to stand up." *Washington Post* (April 7, 2022). https://www.washingtonpost.com/opinions/2022/04/07/ignatius-russia-ukraine-heavy-weapons/.

Kendall-Taylor, Andrea, and Michael Kofman. 2022. "Russia is down. But it's not out." *New York Times* (June 2, 2022). https://www.nytimes.com/2022/06/02/opinion/russia-ukraine-war-nato.html.

Sanger, David E. 2022. "Behind Austin's call for a 'weakened' Russia, hints of a shift." *New York Times* (April 25, 2022). https://www.nytimes.com/2022/04/25/us/politics/ukraine-russia-us-dynamic.html.

The Economist. 2022. "History will judge Vladimir Putin harshly for his war." *The Economist* (February 26, 2022). https://www.economist.com/leaders/2022/02/26/history-will-judge-vladimir-putin-harshly-for-his-war.

Troianovski, Anton, and David E. Sanger. 2022. "Russia issues subtle threats more far-reaching than a Ukraine invasion." *New York Times* (January 16, 2022). https://www.nytimes.com/2022/01/16/world/europe/russia-ukraine-invasion.html.

Wertheim, Steven. 2022. "Can America really envision World War III?" *New York Times* (December 2, 2022). https://www.nytimes.com/2022/12/02/opinion/america-world-war-iii.html.