INTERNATIONAL STUDIES CENTER

JOURNAL

*The International Studies Center (ISC) publishes articles on diplomacy and international affairs in its Journal. The views expressed are the authors' own and do not represent those of the Royal Thai Government or the Ministry of Foreign Affairs of Thailand. Permission to reproduce the article(s) may be obtained from the ISC at isc@mfa.go.th, and due recognition to the author(s) should also be given as appropriate.*

No. 3/2026 | July 2026

# The Misleading Analogy of Cyberwar:
## *Recalibrating the War Frame of Cyber Operations*

***Panutad Watcharaporn***[1]

## 1. INTRODUCTION

For years, cyberspace has emerged as a critical new domain for states' interaction. Past incidents, such as the 2007 Estonia cyberattack[2], the discovery of Stuxnet in 2010[3], and the use of cyber capabilities in the Russia–Ukraine war from 2022[4], have shown how cyberspace is used or exploited in relation to interstate conflict.

Concerns about states using their cyber capabilities to pursue political goals were raised quite early, with many drawing analogies to war. Writing in 1993, John Arquilla and David Ronfeldt of the RAND Corporation declared that "cyberwar is coming," warning that future warfare might take place within an information sphere that "depends less on the geographic terrain than on the nature of the electronic cyberspace."[5] War analogies were soon taken up on the

---

[1] Master of National Security Policy, Australian National University

[2]. "Estonian Denial of Service Incident," Cyber Operations Tracker, Council on Foreign Relations, accessed January 11, 2026, https://www.cfr.org/cyber-operations/estonian-denial-service-incident.

[3]. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," Wired, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[4] . Marcus Willett, "The Cyber Dimension of the Russia–Ukraine War," Survival 64 (2022): 7–26, doi:10.1080/00396338.2022.2126193.

[5]. John Arquilla and David Ronfeldt, "Cyberwar is Coming!" Comparative Strategy 12, no. 2 (Spring 1993): 141–165, RAND Corporation, https://www.rand.org/pubs/reprints/RP223.html.

policymaker side as well. In 2006, Michael Wynne, then US Air Force Secretary, described cyberspace as a domain in which the Air Force "flies and fights," a "domain on a par with land, air, space and sea."[6] In 2011, Leon Panetta, then director of the CIA and later Secretary of Defense, warned of a potential "Cyber Pearl Harbor"—a hypothetical attack that would cause devastating kinetic impact akin to the Japanese strike of 1941.[7] The common theme of these analogies is to characterise the use of cyber capabilities as "traditional war by other means."

These analogies are, however, frequently misleading. Thomas Rid argued that claims about cyberwar are exaggerated, because cyberattacks rarely satisfy the core Clausewitzian elements of war—violence, instrumentality, and a political character.[8] While John Stone counters that cyber sabotage could constitute an act of war when they apply force to produce violent effects, even without direct human lethality, the strategic utility of cyber operations remains contested.[9] Erik Gartzke argues that cyberwar lacks the coercive power of conventional warfare and is unlikely to lead to conquest;[10] Adam Liff likewise concludes that cyberwar functions only within limited circumstances and is unlikely to become an "absolute weapon."[11]

However, the key question is not whether cyber war counts as war in categorical terms, but when the war frame clarifies state behaviour and when it distorts it. Three developments make a more calibrated answer possible. Firstly, International lawyers have converged on an effects-based

---

[6]. Michael W. Wynne, "Cyberspace as a Domain In Which the Air Force Flies and Fights" (C4ISR Integration Conference, Crystal City, VA, November 2, 2006), https://www.airandspaceforces.com/PDF/SiteCollectionDocuments/Reports/2006/November/Day03/Wynne110206.pdf.

[7]. Jason Ryan, "CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor," ABC News, February 11, 2011, https://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905.

[8]. Thomas Rid, "Cyber War Will Not Take Place," Journal of Strategic Studies 35, no. 1 (2012): 5–32, doi:10.1080/01402390.2011.608939.

[9]. John Stone, "Cyber War Will Take Place!," Journal of Strategic Studies 36, no. 1 (2013): 101–108, https://doi.org/10.1080/01402390.2012.730485.

[10]. Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," International Security 38, no. 2 (2013): 41–73, http://www.jstor.org/stable/24480930.

[11]. Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," Journal of Strategic Studies 35, no. 3 (2012): 401–428, https://doi.org/10.1080/01402390.2012.663252.

threshold. Michael Schmitt's "scale and effects" test, codified in the *Tallinn Manual 2.0,* that treats "use of force" as a graded rather than a binary property of an operation.[12] Secondly, Strategic theorists, through cyber persistence theory, have argued that cyberspace rewards exploitation rather than coercion and structurally channels competition *below* the threshold of armed conflict.[13] And lastly, a growing body of empirical work finds that cyber operations are, in practice, far less escalatory than early "Cyber Pearl Harbor" rhetoric assumed.[14]

This article argues that cyberwar should not be *simply* considered "traditional war by other means." Three reasons structure the argument. First, examining the relevance of cyberattacks within the context of war shows that cyberattacks alone cannot serve the whole purpose of warfare. Second, the war paradigm does not fit the nature of cyberspace. Third, treating states' interactions in cyberspace through a binary war–peace paradigm misrepresents those interactions and risks unnecessary escalation. The article suggests that most state use of cyber capability is better understood as a form of statecraft—like economic coercion or diplomacy—that secures state interests in peace and war alike.

To illustrate the argument above, this essay is divided into seven sections. The first section is introduction. The second section develops a working definition of "cyberwar." The third section explains why cyberattacks alone cannot serve the whole purpose of warfare. The fourth section explains why the war paradigm fits poorly with the actors and purposes that characterise cyberspace, deepening the analysis of non-state and proxy actors. The fifth section sets out the

---

[12]. Michael N. Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017), rules 69 and 71; Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," Columbia Journal of Transnational Law 37 (1999): 885–937.

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

[14]. Erica D. Lonergan and Shawn W. Lonergan, Escalation Dynamics in Cyberspace (New York: Oxford University Press, 2023); Benjamin Jensen, Brandon Valeriano, and Sam Whitt, "How Cyber Operations Can Reduce Escalation Pressures: Evidence from an Experimental Wargame Study," Journal of Peace Research 61, no. 1 (2024): 119–136.

suggested framework and recasts most cyber activity as statecraft. section raises concerns over the potential risks of state leaders characterising cyberattacks as warfare, which may result in disproportionate responses and risk unnecessary escalation of conflict. The last section concludes

## 2. DEFINING CYBERWAR

There is still no universally accepted definition of "cyberwar," and definitions suggested by academics still vary to some degree. The principal difference is whether to emphasise the perceived *strategic outcome* for states, the physical kinetic *damage* an operation might cause, or the *legal* threshold an operation crosses.

In the early "cyberwar debate," Arquilla and Ronfeldt broadly defined the term as an attempt to gain advantage in "information and knowledge" by disrupting an opponent or gaining information for oneself, and specified that the concept applies to conflicts between states.[15] This definition is in line with Thomas Rid's work, which includes information gathering activities such as espionage within the field of analysis.[16] Such definitions emphasise cyberspace as a *means* to an end and downplay kinetic damage from the operation itself.

A second view focuses on *damage*. Clarke and Knake define cyberwar as "action by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption."[17] The RAND Corporation similarly defines it as "actions by a nation-state or international organisation to attack and attempt to damage another nation's computers or information networks."[18]

---

[15]. Arquilla and Ronfeldt, "Cyberwar is Coming!"
[16]. Rid, "Cyber War Will Not Take Place."
[17]. Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It (New York: Ecco, 2010).
[18]. "Cyber Warfare," RAND Corporation, accessed January 11, 2026, https://www.rand.org/topics/cyber-warfare.html.

A third group of definitions, developed by international lawyers, fixes on the *legal threshold* an operation cross. The *Tallinn Manual 2.0* holds that a cyber operation amounts to a prohibited "use of force," and may rise to an "armed attack" triggering the right of self-defence, when its "scale and effects" are comparable to those of a kinetic operation of equivalent magnitude. Schmitt's qualitative criteria – severity, immediacy, directness, invasiveness, measurability of effects, military character, and degree of state involvement – supply the metric, and a number of states, including Germany, have adopted the scale-and-effects approach in their national positions.[19] This legal perspective is important because it treats "cyberwar" as a matter of degree rather than a simple yes-or-no category, as majority of state cyber activity falls *below* the use-of-force line altogether, in a space that Lucas Kello aptly calls "unpeace," neither war nor genuine peace.[20]

From this variation, two features of the standard concept can be drawn. First, "cyberwar" is highly state-centric, as most definitions place state actors at the origin and, preferably, the endpoint of the operation. Second, it concerns the use of cyber capabilities, often referred to as "cyberattack," as a means to pursue their goals. This article therefore uses "cyberwar" to mean *the use of cyber capabilities, specifically cyberattacks, by state actors to pursue their objectives*. However, this label covers activities that vary widely in severity and coercive legibility. Treating all of them as one category of "war" is therefore the main analytical mistake this article seeks to correct.

---

[19]. Schmitt, ed., Tallinn Manual 2.0, rules 69, 71, and 80; on emerging state practice see Michael N. Schmitt, "The Use of Cyber Force and International Law," in The Oxford Handbook of the Use of Force in International Law, ed. Marc Weller (Oxford: Oxford University Press, 2015).

[20]. Lucas Kello, The Virtual Weapon and International Order (New Haven: Yale University Press, 2017).

## 3. CYBERATTACK AND TRADITIONAL WAR

Cyberwar should not be simply considered “traditional war by other means” because cyberattacks alone cannot serve the whole purpose of war. They fall short of producing the political outcome or coercive effect that is the ultimate object of warfare, for at least two reasons.

First, cyberattacks usually come with an "attribution problem," in which it is difficult to identify the actor who conducted an attack. This renders any message or signal from the attacker unclear and leaves the target uncertain how to respond. As Robert Jervis argued, perception and communication are essential to how states influence one another, and “signalling often fails when the perceiver does not understand what message the actor is trying to communicate.”[21] The point can be sharpened through coercion theory. Erica Borghard and Shawn Lonergan note that successful coercion requires clearly communicated threats, a credible capability, and reassurance that compliance will end the pain, conditions that covert, deniable, and technically reversible cyber operations are no designed to meet.[22] If a state cannot prove who conducted an attack, it cannot read the political demand behind it, and without a legible demand there is no coercion.

Second, cyberspace is not a standalone sphere by its nature, which makes it unlikely that cyberwar could constitute a self-sufficient form of warfare. The damage inflicted by a cyberattack tends to be temporary and falls short of being comprehensive without the involvement of other instruments of war. Even the most sophisticated purely cyber operation such as Stuxnet only slowed Iran’s enrichment process and produced no politically decisive outcome of the kind warfare

---

[21]. Robert Jervis, “Signaling and Perception: Drawing Inferences and Projecting Images,” in Political Psychology, ed. Kristen Renwick Monroe (Mahwah, NJ: Lawrence Erlbaum Associates, 2002), 304.

[22]. Erica D. Borghard and Shawn W. Lonergan, “The Logic of Coercion in Cyberspace,” Security Studies 26, no. 3 (2017): 452–481, https://doi.org/10.1080/09636412.2017.1306396.

seeks.[23] Lower-intensity operations, such as the distributed denial-of-service (DDoS) campaign against Estonia in 2007, are reversible and unlikely to compel concessions.[24]

Instead, cyberattacks are most effective in support of kinetic warfare rather than as a replacement for it. Operation Orchard in 2007, in which Israeli cyber units fed Syrian air-defence radars a false "clear sky" to enable an air raid, illustrates cyber as a tool of sabotage at the tactical and operational level rather than the strategic level.[25] This supports Gartzke's image of cyber as an "artillery barrage" that "clears enemy trenches but still requires the infantry and other arms to achieve breakout."[26] The Israeli operation did not destroy the suspected reactor; it merely opened the door for the aircraft. The Russia–Ukraine war reinforces the point on the largest contemporary canvas. Despite pre-war expectations of a decisive "cyber blitz," most assessments conclude that cyber operations have been a supporting instrument whose effects, dramatic when imagined in peacetime, receded in significance amid high-intensity kinetic combat.[27]

Two objections must be confronted here. The first, pressed by Stone and by Herbert Lin, is that cyber operations *can* cross into force and violence at the high end, as code that opens a dam's floodgates or disables a hospital's life-support systems would produce death and destruction indistinguishable, in their effects, from a kinetic strike.[28] The second objection is that the violence of war was never exclusively physical in the first place. A naval blockade, for instance, is treated as an act of war even though it does not rely directly on bloodshed. Instead, it cuts off food, fuel,

---

[23]. Rid, "Cyber War Will Not Take Place."
[24]. "Estonian Denial of Service Incident."
[25]. "Attack on Syrian Air Force," Cyber Operations Tracker, Council on Foreign Relations, accessed January 12, 2026, https://www.cfr.org/cyber-operations/attack-syrian-air-force.
[26]. Gartzke, "The Myth of Cyberwar," 57.
[27]. Willett, "The Cyber Dimension of the Russia–Ukraine War"; see also the lessons-learned consensus surveyed in "Cyber in War: Lessons from the Russia–Ukraine Conflict," Lieber Institute, West Point, 2023.
[28]. Stone, "Cyber War Will Take Place!"; Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," Journal of National Security Law & Policy 4, no. 1 (2010): 63–86.

and military supplies until the adversary's capacity and will begin to collapse.[29] If this kind of non-kinetic pressure can count as war, then the absence of explosions alone cannot exclude cyber operations from the category

These objections show that the right question is not *whether* harm is kinetic but *whether an operation crosses a threshold of scale and effects while carrying a legible coercive purpose*. What blockade or economic statecraft possesses, and what cyber operations characteristically lack, is instructive. A blockade is openly declared and unmistakably attributed; it is effective and continuous, sustained by forces until the demand is met; and its coercive logic is transparent to the target. Cyber operations are typically the opposite and therefore do not fit in the same sense.

## 4. CYBERSPACE AND THE WAR PARADIGM

Cyberwar should not be simply considered "traditional war by other means" because the war paradigm does not fit to apply to the nature of cyberspace for two reasons: its actors and its purposes.

On actors, as mentioned in section two, the concept of cyberwar is highly state-centric, with academics and policymakers often assuming that states are the main actors in this domain. This is because the idea of warfare is based on the Westphalian worldview of International Relations that violence of warfare is only monopolised by states.[30] In reality, the actors in cyberspace are frequently unclear, and states are no longer the sole players. The field includes private firms, organised criminal groups, and hacktivists, and states routinely exploit this plurality by using criminal groups or independent hackers as proxies to gain plausible deniability and specialised skills.

---

[29]. Wolff Heintschel von Heinegg, "Blockade," in Max Planck Encyclopedia of Public International Law (Oxford: Oxford University Press, 2015).
[30]. Bruce D. Porter, War and the Rise of the State: The Military Foundations of Modern Politics (New York: Simon & Schuster, 2002).

These proxy relationships are not all the same as they can be divided into clearer types. Tim Maurer distinguishes three modes by which states relate to non-state cyber actors: *delegation*, in which the state exercises tight control over a contractor or unit acting on its behalf; *orchestration*, in which the state enables and loosely guides an ideologically aligned actor without issuing specific instructions; and *sanctioning*, in which the state simply tolerates through deliberate inaction against activity that serves its interests.[31]

Maurer's typology helps organise the examples that follow by showing how closely each non-state actor is connected to state control. North Korea's Lazarus Group, which conducts financially motivated crime alongside espionage to fund a sanctioned regime, sits near the delegation–orchestration boundary.[32] Russia's cultivation of criminal ransomware groups, recently the target of coordinated US and allied action, exemplifies orchestration shading into sanctioning, where state and criminal motives are deliberately blurred for deniability.[33] The IT Army of Ukraine – volunteers worldwide whom the Ukrainian government called upon to mount DDoS operations against Russian targets after the 2022 invasion – shows a state orchestrating, and partly sanctioning, a civilian force that international humanitarian law struggles to classify.

Even in cases tied directly to inter-state conflict, the role of non-state actors persists. Hacktivist groups – civilians using cyber tools for their own political goals – have conducted numerous operations connected to inter-state disputes. In the 2023 Israel–Hamas conflict, pro-

---

[31]. Tim Maurer, Cyber Mercenaries: The State, Hackers, and Power (Cambridge: Cambridge University Press, 2018); Tim Maurer, "'Proxies' and Cyberspace," Journal of Conflict & Security Law 21, no. 3 (2016): 383–403.

[32]. Kerstin Zettl-Schabath, Alisa Jazxhi, and Camille Borrett, "Advanced Persistent Threat Profile: Lazarus Group," EuRepoC, February 2024, https://eurepoc.eu/wp-content/uploads/2024/02/Advanced-Persistent-Threat-Profile-Lazarus-February-2024.pdf.

[33]. "Justice Department Announces Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups," Office of Public Affairs, U.S. Department of Justice, December 9, 2025, https://www.justice.gov/opa/pr/justice-department-announces-actions-combat-two-russian-state-sponsored-cyber-criminal; William Akoto, "Secret Cyber Wars," Irregular Warfare Initiative, June 4, 2024, https://irregularwarfare.org/articles/secret-cyber-wars/.

Palestinian and pro-Iranian groups struck Israeli and Gazan infrastructure;[34] the same dynamic appeared in the 2025 Thailand–Cambodia dispute, where groups claiming to act for each state attacked the other's information infrastructure.[35]

States are also not the only targets. The 2014 breach of Sony Pictures was a politically motivated attack on a private company, as North Korean hackers retaliating against the film *The Interview* which mocked Kim Jong-un. This incident challenges the Westphalian view of war, as a nuclear-armed state engaged in a conflict with a movie studio, resulting a blur of line between crime, vandalism, and national security.[36]

However, this does not mean that states have become an irrelevant actor, as they still shape much of the cyber ecosystem. The presence of proxy just further detaches a cyber incident from an identifiable sender and a readable demand, pulling it away from the logic of war and toward the logic of covert statecraft. It also weakens the legal basis for treating the incident as war, since attribution to a state is the precondition for state responsibility and for any lawful forceful response.

On purpose, traditional warfare is understood as kinetic and preferably decisive, whereas cyberattacks are better suited to covert effort. Ben Buchanan argues that cyber operations underperform at overt tasks such as signalling and deterrence but excel at "shaping" a situation and seizing advantage.[37] A state may use espionage to gain leverage in negotiations and bend an agreement toward its preferences. Daniel Kuehl likewise treats cyberspace as an instrument of

---

[34]. Kate Langley, "'Hacktivism', Cyber Warfare, and the 2023 Israel–Hamas Conflict," Young Diplomats Society, November 25, 2023, https://www.theyoungdiplomats.com/post/hacktivism-cyber-warfare-and-the-2023-israel-hamas-conflict.

[35]. "Hacktivist at War: The Cambodia–Thailand Cyber Escalation, July–August 2025," Group-IB, accessed January 12, 2026, https://www.group-ib.com/resources/research-hub/hacktivist-at-war-july-august-2025/.

[36]. Adam Segal, The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (New York: PublicAffairs, 2016), 51–55.

37. Ben Buchanan, The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics (Cambridge, MA: Harvard University Press, 2020).

power that "links to, supports, and enables the creation and exercise of the other instruments," extending influence well beyond cyberspace itself.[38]

Sabotage and destabilisation are a second mode of covert effect. Although Stuxnet produced no decisive political outcome, it helped shape the strategic environment by delaying Iran's programme for years, improving the US negotiating position and buying time.[39] This pattern is exactly what cyber persistence theory predicts. Fischerkeller, Goldman, and Harknett argue that cyberspace is governed by a logic of *exploitation* rather than coercion. Due to the nature that networked actors are in constant contact, advantage accrues to those who persistently exploit vulnerabilities to shift facts on the ground, and the structure of the domain channels this competition into a tacitly "agreed" space below the threshold of armed conflict.[40] On this account, the under-performance of cyber as a coercive instrument is not a contingent weakness but a structural feature of the environment.

Within cyberspace, then, the greatest gains accrue to actors who aggressively shape the geopolitical environment, not to those who hint, threaten, or coerce. Cyberspace is an environment of exploitation more than of coercion, and strategic gains there do not require an opponent's concession.

## 5. CYBER OPERATIONS AS STATECRAFT

If cyberattacks cannot achieve the full objectives of war and the traditional war paradigm does not align with cyberattacks, then how should cyberwar be understood, particularly within the field of International Relations?

38. Quoted in John B. Sheldon, "The Rise of Cyberpower," in Strategy in the Contemporary World, 5th ed., ed. John Baylis, James J. Wirtz, and Colin S. Gray (Oxford: Oxford University Press, 2016), 291–306.
39. Zetter, "An Unprecedented Look at Stuxnet."
40. Fischerkeller, Goldman, and Harknett, Cyber Persistence Theory.

This article suggests that state use of its cyber capability should be considered as a form of statecraft – like economic coercion or diplomacy – deployed to secure state interests both in peace and in war.

As Richard Harknett and Max Smeets observe, cyber operations can function as an alternative to warfare.[41] Cyber cannot fully replace physical force, but it offers states a way to pursue advantage while avoiding all-out war. The very features identified above – limited kinetic violence and unclear attribution – are exploited by states to act against rivals while remaining below the threshold of war. The option is especially attractive to weaker states as cyberspace imposes lower logistical demands, and an unsophisticated operation such as DDoS is cheap yet can impose disproportionate cost. Cyber capability serves strategic ends across the conflict spectrum. During peacetime through espionage and the theft of adversaries' know-how and during war through tactical effects such as disabling an electrical grid or penetrating command-and-control. As John Sheldon puts it, cyber power is "the ability, in peace, crisis, and war, to exert prompt and sustained influence in and from cyberspace."[42]

These observations can be organised into a framework with two variables. The first is the *severity of effects* such as how far the operation moves along a ladder from non-destructive exploitation (espionage), through reversible disruption (defacement, DDoS), to functional or physical degradation (Stuxnet), and finally to destruction whose scale and effects approach those of a kinetic attack. This axis tracks the jus ad bellum thresholds of the *Tallinn Manual* and Lin's distinction between cyber-exploitation and cyber-attack. The second variable is *coercive legibility*, which is the degree to which the operation is attributable to an identifiable sender and carries a

---

[41]. Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," Journal of Strategic Studies 45, no. 4 (2022): 534–567, https://doi.org/10.1080/01402390.2020.1732354.

[42]. Sheldon, "The Rise of Cyberpower," 291–306.

communicated demand, the conditions coercion theory requires. Proxy mediation, deniability, and reversibility push an operation toward the *opaque* pole, while open declaration and an explicit demand push it toward the *legible* pole.

Crossing the two axes yields four regions, summarised in Table 1. The crucial claim is that an operation behaves like *war* – coercive, and properly governed by the law and logic of armed conflict – only in the upper-right region, where severe effects meet a legible demand. Empirically, that region is nearly empty, as no cyber operation to date is widely agreed to have crossed the armed-attack threshold. The mass of real-world activity sits in the other three regions, for which "war" is the wrong description.

**Table 1.**

| | **Opaque Legibility**<br><br>(deniable, proxy-mediated, no clear demand) | **Legible Legibility**<br><br>(attributable, explicit demand) |
|---|---|---|
| **High Severity**<br><br>(degradation/destruction) | **II – Deniable Sabotage**<br><br>high-severity yet deliberately deniable politically and legally | **I – Coercive Force**<br><br>Hypothetical critical-infrastructure attack causing death, with coercive declaration from the state responsible for the attack. |
| **Low Severity**<br><br>(espionage/disruption, reversible) | **III – Covert Shaping**<br><br>no physical damage, opaque in legibility, aimed at information advantage rather than concession | **IV – Demonstrative Signalling**<br><br>Attributable in a rough sense and politically expressive, but low in severity and coercively weak. More likely to be treat as a public-order or diplomatic matter. |

Reading the article's cases through Table 1 clarifies them. The SolarWinds compromise, in which Russian operators tampered with software updates to infiltrate US agencies and exfiltrate data, sits firmly in Region III with low in severity (no physical damage), opaque in legibility, and aimed at information advantage rather than concession. It is espionage, an instrument of statecraft, not war.[43] The 2007 Estonia DDoS attack case sits in Region IV which is attributable in a rough sense and politically expressive, but low in severity and coercively weak. Stuxnet case occupy Region II with its genuinely high-severity yet deliberately deniable politically and legally. Region I is the analytically and politically hardest case to found, as to date there has been no instance of a highly destructive cyber incident accompanied by an explicit, coercive declaration from the state responsible for the operation.

According to the suggested frame work, Rid is right about Regions III and IV, where most activity lives. Stone and Lin are also right about Region I, and about the upper edge of Region II, where effects can rival those of force. While the analogy of cyberwar misleads not because it is always wrong but because it is applied uniformly to a space in which it is only true in a very limited case which also haven't happened yet.

## 6. MISPERCEPTION, ESCALATION, AND THE CASE FOR CALIBRATED RESTRAINT

Treating states' interactions in cyberspace through a binary war–peace paradigm misrepresents those interactions and can lead to misperception, disproportionate responses, and unnecessary escalation.

[43]. On treating cyber espionage as below the use-of-force threshold, see Schmitt, ed., Tallinn Manual 2.0, rules 32 and 69.

Three sources of misperception follow from generalising every use of cyber capability as "warfare." First, it misses the point of much cyber activity, which is often an alternative a state chooses *instead* of all-out war.[44] Second, cyber capabilities are not used exclusively in wartime. States use them more in peacetime, as statecraft for pursuing advantage below the threshold of war. Third, not every cyber offensive should count as war. Espionage operation, for example, is the equivalent of intelligence-gathering or reconnaissance, traditionally below that threshold. The SolarWinds operation likely affected US national security, yet aimed to gain information advantage without breaking anything physically or triggering a military response. The difficulty lies in the target's determination, since the real intent behind any single operation and its place in a wider campaign is rarely clear at the moment of detection.

Whether this ambiguity is dangerous is contested. Robert Jervis and Jason Healey, holds that cyber conflict is acutely escalation-prone – opaque, fast, offence-dominant, and difficult to control once under way – and warns that strategies of persistent engagement may court inadvertent escalation.[45] If that were generally true, a war-framing of cyberspace might be prudent insurance. Yet the accumulating empirical record points the other way. Erica and Shawn Lonergan find that the inherent limitations of cyber operations have suppressed both intentional and inadvertent escalation. Experimental wargames by Jensen, Valeriano, and Whitt show that the availability of a cyber option can *reduce* escalation pressure by offering decision-makers a non-violent off-ramp. Studies by Valeriano and Maness also find cyber conflict to be restrained, regional, and low intensity.[46]

---

[44]. Borghard and Lonergan, "The Logic of Coercion in Cyberspace"; Shaun Riordan, Cyberdiplomacy: Managing Security and Governance Online (Cambridge: Polity Press, 2019).

[45]. Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," Journal of Cybersecurity 5, no. 1 (2019): 1–15.

[46]. Lonergan and Lonergan, Escalation Dynamics in Cyberspace; Jensen, Valeriano, and Whitt, "How Cyber Operations Can Reduce Escalation Pressures"; Brandon Valeriano and Ryan C. Maness, Cyber War versus Cyber Realities: Cyber Conflict in the International System (New York: Oxford University Press, 2015).

The suggested framework reconciles these findings. Escalation danger is not uniform across cyberspace, but rather concentrates in Region II, where high-severity but deniable operations tempt a targeted state to over-attribute and over-respond. In Regions III and IV, where the great majority of activity occurs, the same opacity and reversibility that frustrate coercion also *dampen* escalation, which is why the empirical record looks comparatively calm.

Critics may argue that loosening the 'war frame' around cyber operations removes essential restraints, as traditional use-of-force thresholds and red lines keep state competition in check. While this framework is valuable, it shouldn't be applied to every cyber incident. The solution this article suggests is calibration, not abandonment. The traditional rules of war should still apply to severe, destructive attacks against critical infrastructure (Region I and upper Region II). However, states should also avoid treating lower-level espionage and disruptions as acts of war, as doing so would only spikes political tensions and increases the risk of a overreaction.

Red lines are credible only when used sparingly. If a state treats every minor intrusion as an act of war, it devalues the very boundaries it needs others to respect. The 2007 Estonia case illustrates the stakes. Had Estonia, a NATO member, characterised the DDoS campaign as an armed attack, it might have invoked Article 5 collective defence over what was, in effect, temporary website disruption, which definitely is an escalation disproportionate to the harm.[47] Distinguishing cyber vandalism from war is therefore vital to stability. Yet the same logic gives states good reason to declare, clearly and credibly, the narrow class of effects that they *will* treat as armed attacks.

[47]. “Estonian Denial of Service Incident.”

## 7. CONCLUSION

This article has examined the war analogies often used to describe cyber conflict and argued that the analogy is miscalibrated. Three arguments support the reframing. First, cyberattacks alone cannot serve the whole purpose of warfare because they struggle to send a legible signal of the attacker's demand and depend on uncertain perception, and because cyberspace is not a standalone sphere, therefore cyberwar cannot stand without contribution from other forms of warfare, as the supporting role of cyber in the Russia–Ukraine war confirms. Second, the war paradigm centres on state actors and decisive effects, whereas cyberspace is thick with non-state and proxy actors, and rewards covert shaping and exploitation over decisive force. Third, treating cyber activity through a war mentality invites disproportionate responses to what is often a deliberate alternative to war.

This article's contribution lies in converting these observations into a calibrated framework. Mapping cyber operations by their severity and coercive legibility reveals that the 'war frame' applies only to a narrow subset of severe, overtly coercive acts. In contrast, the vast majority of state cyber activity falls into a low-severity, deniable region that does not meet the threshold of warfare.

Ultimately, most state cyber activity is an instrument of statecraft – much like diplomacy or economic coercion – used continuously across peace and war time. Acknowledging this does not weaken our defences against truly destructive attacks. Instead, it allows policymakers to move beyond the binary of 'war' and 'not war.' By calibrating our frameworks, we can reserve the heavy machinery of armed conflict for the severe impacts that require it, while addressing broader cyber competition through the stabilising lens of foreign policy.