

Comparing the long-term outcomes of historical US preemptive operations such as Stuxnet, Operation Glowing Symphony, and Russian grid malware, do these precedents demonstrate a stable deterrence framework or a slippery slope toward uncontrolled escalation?

September 9, 2026 | SnugLab Research

Executive Summary

The long-term outcomes of historical US preemptive operations such as Stuxnet, Operation Glowing Symphony, and Russian grid malware primarily indicate a **slippery slope toward uncontrolled escalation** rather than a stable deterrence framework. Evidence suggests these precedents have led to increased cyber capability proliferation, persistent low-level "grey zone" conflicts, and heightened uncertainty regarding intent and red lines [1, 2, 6, 7, 8, 9]. While cyber operations can offer de-escalatory alternatives and resilience strategies provide a path to greater stability, these mitigating factors have not prevented an overall trajectory of escalating cyber activity and risk.

Key Findings

Proliferation and Retaliation Accelerate Escalation

The deployment of offensive cyber tools has demonstrably led to capability diffusion and retaliatory actions, contributing to a slippery slope of escalation. The Stuxnet malware, first uncovered in June 2010, became publicly known and reusable, allowing other attackers to modify and exploit its code [1, 5, 9]. Following this, Iran reportedly fortified its cyber warfare capabilities and launched retaliatory strikes, including attacks against US banks between 2012 and 2013, the Shamoon attack against Saudi Aramco in 2012, and a strike against Las Vegas Sands Corporation in 2014 [2, 9]. This pattern demonstrates that deploying cyber weapons can inadvertently disseminate their intellectual property, escalating capabilities beyond the initial target and exposing the initiator to similar attacks [1].

Persistent Gray-Zone Conflict and Escalating Frequency

The operations illustrate a normalization of sustained infrastructure degradation within a "grey zone" below the threshold of traditional armed conflict, which has not led to stable deterrence but rather to continuous, low-level conflict. Russian grid malware operations, for instance, caused significant civilian impact, leaving over 200,000 people without power for several hours in December 2015 and cutting electricity to between 100,000 and 200,000 residents of Kyiv in December 2016 [4, 12]. This persistent shadow warfare is exemplified by the rapid increase in Russian attacks in Europe, which quadrupled between 2022 and 2023, and nearly tripled between 2023 and 2024 [11]. This escalating frequency suggests that existing deterrence strategies are failing to coerce adversaries, reinforcing a slippery slope toward continuous hostility [11].

Ambiguity and Blurred Lines Increase Miscalculation Risks

The increasing indistinguishability between offensive and defensive cyber operations, coupled with doctrines like "persistent engagement," contributes to crisis instability by making it difficult for adversaries to discern intent [16]. This ambiguity forces worst-case interpretations and increases the likelihood of incidents that degrade strategic stability [16]. Furthermore, the integration of cyber disruptions directly into hybrid warfare campaigns blurs the causal link between digital disruption and physical damage, systematically lowering the threshold for wider conflict. During Russia's 2022 invasion of Ukraine, cyberattacks were launched simultaneously with kinetic operations, such as a missile strike on a Kyiv television tower and the penetration of Ukraine's nuclear power company network [8]. Preemptive operations, like Operation Glowing Symphony, also deliberately induce confusion to trigger kinetic responses, as it caused technical errors in ISIS networks to force operators into using less secure tools, revealing their physical locations for kinetic targeting [15].

Instability of Deterrence-by-Punishment Due to Attribution Gaps

Deterrence-by-punishment is inherently unstable in cyberspace due to attribution challenges and "grey zone" ambiguity, which allow adversaries to conduct persistent hostile activities without provoking decisive retaliation [2, 10, 14]. While US operations like Stuxnet and Operation Glowing Symphony were successfully attributed to the United States and its allies [1, 3, 9, 15], this transparency makes them vulnerable to direct retaliation, as seen with Iran's cyber responses [2, 9]. In contrast, Russia strategically

exploits anonymity and uses proxies to maintain operational ambiguity, enabling it to evade the costs of punishment and weaken deterrence-by-punishment strategies [2, 10, 11, 14]. This disparity contributes to a continuous low-level conflict rather than a stable deterrence model [2, 10, 11].

Mitigating Factors and Alternative Approaches Offer Limited Stability

Despite the overall trajectory toward escalation, some factors suggest elements of stability or alternative pathways. Cyber operations can serve as a "less costly alternative to conflict" and have been used to de-escalate situations, such as the 2019 US cyberattack on Iran substituting for a conventional air strike [1, 13]. Analysts note that cyberattacks have "never escalated a conflict into the kinetic domain" [1, 13]. Additionally, "deterrence by denial" through robust resilience strategies, such as hardening critical infrastructure and implementing a "total defense" strategy, offers a more stable approach than relying solely on threats of punishment [2, 7]. Operations like Glowing Symphony also indicate a maturation of US cyber capabilities and processes, which could lead to more controlled and effective use of cyber tools [2, 3]. However, the limited concrete evidence for long-term compliance with established cyber red lines following US preemptive operations suggests that these mitigating factors have not yet established a stable deterrence framework [17].

Implications

The precedents indicate that offensive cyber operations, while offering tactical advantages and sometimes serving as de-escalatory alternatives to kinetic force, have not fostered a stable deterrence framework. Instead, they have contributed to a dynamic of continuous low-level conflict, capability proliferation, and increased strategic ambiguity. For global security, this implies a future characterized by persistent "grey zone" competition, where states and non-state actors engage in ongoing cyber hostilities below the threshold of traditional warfare. The blurring of lines between espionage, pre-positioning, and active disruption, coupled with the difficulty of attribution, means that miscalculation and unintended escalation remain significant risks. The emphasis on resilience and deterrence by denial will likely grow as states seek to mitigate the impacts of these pervasive threats, but this alone may not be sufficient to prevent a gradual slide toward more severe cyber-physical conflicts.

Limitations and Caveats

The assessment of long-term outcomes in cyberspace is inherently complex due to the evolving nature of technology, the difficulty of definitive attribution, and the challenge of proving causation for deterrence or escalation. While quantitative metrics like centrifuge destruction, power outages, and attack frequency provide concrete evidence of impact and proliferation, the precise thresholds for "uncontrolled escalation" remain subject to interpretation. The absence of kinetic escalation following specific cyberattacks does not definitively prove a stable deterrence framework, as it could also reflect a calculated decision by adversaries to avoid immediate kinetic retaliation while pursuing long-term cyber objectives. Furthermore, the analysis relies on publicly available information, which may not fully capture the classified aspects of these operations or the full scope of their long-term consequences.

Sourcing audit. A check of this report's claims against the source material it was written from could not trace 8 of 11 claims back to a passage in that material. Treat the specific figures and findings above as unverified pending a re-run with a wider source pool.

Sources

- [1] [edu] Stuxnet - cisac.fsi.stanford.edu - <https://cisac.fsi.stanford.edu/news/stuxnet>
- [2] [edu] Viewcontent.Cgi - digitalcommons.usf.edu - <https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=2361&context=jss>
- [3] [edu] Uscybercom After Action Assessments Operation Glowing Sympho - nsarchive.gwu.edu - <https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscycbercom-after-action-assessments-operation-glowing-symphony>
- [4] [edu] Viewcontent.Cgi - digitalcommons.unl.edu - <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=3118&context=nlr>
- [5] [edu] Stuxnet Digital Staff Ride - mwi.westpoint.edu - <https://mwi.westpoint.edu/stuxnet-digital-staff-ride/>
- [6] Cyber Risk Manipulation A Powerful Tool For U S Offensive Op - gssr.georgetown.edu - <https://gssr.georgetown.edu/the-forum/topics/intel-natsec/cyber-risk-manipulation-a-powerful-tool-for-u-s-offensive-operations/>
- [7] [edu] Why The Us Needs A Total Defense Strategy Based On Resilienc - brookings.edu - <https://www.brookings.edu/articles/why-the-us-needs-a-total-defense-strategy-based-on-resilience/>
- [8] [edu] Technology Complexity Uncertainty And Deterrence - kissinger.sais.jhu.edu - <https://kissinger.sais.jhu.edu/programs-and-projects/kissinger-center-papers/technology-complexity-uncertainty-and-deterrence/>
- [9] [wiki] Stuxnet - en.wikipedia.org - <https://en.wikipedia.org/wiki/Stuxnet>
- [10] War Without End Deterring Russias Shadow War - cepa.org - <https://cepa.org/comprehensive-reports/war-without-end-deterring-russias-shadow-war/>
- [11] Russias Shadow War Against West - csis.org - <https://www.csis.org/analysis/russias-shadow-war-against-west>
- [12] Cyber Effects In Warfare Categorizing The Where What And Why - tnsr.org - <https://tnsr.org/2024/08/cyber-effects-in-warfare-categorizing-the-where-what-and-why/>

- [13] [ngo] The Potential Human Cost Of Cyber Operations - icrc.org -
<https://www.icrc.org/en/download/file/97346/the-potential-human-cost-of-cyber-operations.pdf>
- [14] Strategic Stability Cyber Operations And International Secur - cigionline.org -
<https://www.cigionline.org/articles/strategic-stability-cyber-operations-and-international-security/>
- [15] Operation Glowing Symphony (2016 - cyberlaw.ccdcoe.org -
[https://cyberlaw.ccdcoe.org/wiki/Operation_Glowing_Symphony_\(2016](https://cyberlaw.ccdcoe.org/wiki/Operation_Glowing_Symphony_(2016)
- [16] Cyber Doctrines And Risk Nuclear Crisis Instability Part 1 I - cfr.org -
<https://www.cfr.org/articles/cyber-doctrines-and-risk-nuclear-crisis-instability-part-1-issues-us-cyber-strategy>
- [17] [edu] Us Cyber Deterrence Bringing Offensive Capabilities Into The - jfsc.ndu.edu -
<https://jfsc.ndu.edu/Media/Campaigning-Journals/Academic-Journals-View/Article/3149856/us-cyber-deterrance-bringing-offensive-capabilities-into-the-light/>