Hacking the Apocalypse: How Cyberattacks Could Trigger Nuclear Escalation

by
Gilles A. Paché

Many of the world's strategists still share the same conviction: as Kathryn Bigelow's film *A House of Dynamite* (2025) dramatizes, nuclear escalation can only originate from a missile of unknown origin heading straight for Chicago. Yet, this old "Cold War" vision no longer seems entirely relevant. As cyberattacks target critical infrastructure, a long-taboo question arises: how far can we tolerate digital offensives that paralyze a country or manipulate an election before considering a nuclear response? What if the most dangerous attack to unfold in the late 2020s originates not from a silo, but from a single line of code?

Cyber Shockwaves

Imagine a simple piece of computer code shutting down nuclear power plants, paralyzing transportation networks, and disrupting vital military systems. For more than a decade, cyberattacks against critical infrastructure have been more than just intrusions; they can have effects comparable to those of conventional acts of war, and threatening global stability. For nuclear democracies, the question has become crucial: at what point does a digital incident cross the threshold of severity required to trigger deterrence calculations, or even justify a nuclear response?

Cyberspace is now a theater of constant confrontation where adversaries seek to undermine each other's trust, disrupt economies, and test resilience. This invisible competition weakens traditional deterrence mechanisms, which rely on clear signals. In cyberspace, nothing is clear, with uncertain effects and often unintentional escalation. Yet, the potential damage of a sophisticated cyberattack against an electrical grid or supply chains could exceed that of a conventional bombing. The problem stems from three major developments.

Critical Weak Spots

The first development is the *increasing vulnerability of critical infrastructure*, whose technical complexity creates countless points of weakness. Hospitals, refineries, water distribution systems, and railway networks rely on technologies that are sometimes outdated and rarely protected against determined state and non-state actors. A coordinated and simultaneous attack against multiple sectors could severely paralyze a country for weeks to months, causing economic chaos and widespread social disruption.

The second development concerns the *strong integration of cyberspace and nuclear power*. Command, control, and communication systems have become more digital than ever, and thus more exposed to cyberattacks. Even a non-destructive intrusion, subtly targeted and difficult to detect, could be interpreted as an attempt to undermine the capacity to retaliate. In such cases, the precise or approximate perception of risk becomes as dangerous as the attack itself, amplifying the potential for misunderstandings and unintentional escalation.

The third development, finally, is the *bolder behavior of adversaries of democratic regimes*, who use cyberspace as a tool for exerting pressure without incurring significant costs. Who would doubt that Russia, China, North Korea, and Iran regularly demonstrate their ability to disrupt the institutions of democratic regimes? The relative success of their operations encourages them to push the boundaries even further, as they are aware of the existence of a "gray zone" where traditional deterrence does not fully apply.

These major transformations lead to a fundamental question: should democracies clarify as quickly as possible that certain cyberattacks could cross a threshold triggering a major military response, including nuclear? The objective of a new doctrine would then not be to lower the nuclear threshold, but to re-establish a credible and robust level of deterrence. Because if adversaries believe that cyberattacks are "zero-cost," they will continue to systematically target vital infrastructure, exploiting critical vulnerabilities with impunity and minimal risk to themselves.

Strategic High Stakes

A first argument for clarifying the doctrine rests on proportionality: a massive cyberattack targeting critical infrastructure could have consequences comparable to a bombing. In this context, it would be consistent to specify that the response is not limited to conventional means. Analysts point out that U.S. nuclear doctrine already considers the possibility of devastating consequences from non-nuclear strategic attacks, and they believe that the nuclear threat is not explicitly excluded, even if the *no-first-use* scenario remains dominant.

A second argument concerns strategic stability. Today, adversaries regularly stress the defenses of democratic regimes in the "gray zone," without immediate risk of escalation. Clarifying the rules of engagement and explicitly integrating cyberspace into strategic thinking could strengthen deterrence and limit adversarial gambles in this gray zone. The United States, the United Kingdom, and France could thus reduce uncertainty regarding the potential consequences of sophisticated cyberattacks, one form of irregular warfare, while emphasizing that any major offensive would have significant repercussions.

A third argument concerns the protection of nuclear command. Even a limited attack on control systems could be interpreted as an attempt to neutralize the second-strike capability, creating an extreme risk of miscalculation, especially with the increasing use of artificial intelligence. By clearly announcing that such an intrusion would be considered a serious and unacceptable act, democratic regimes would strengthen their strategic stability, discouraging any hostile action and reducing the risk of unintentional escalation during times of international crisis.

Perilous Lines

This doctrinal shift, however, carries significant risks, notably the unintentional lowering of the nuclear threshold. Even if the clarification primarily aims to strengthen deterrence, it could be perceived as an excessive threat by non-democratic States, prompting them to rapidly modernize their nuclear arsenals or develop sophisticated offensive cyber capabilities. The proliferation of

cyber threats with potentially physical effects creates a low-profile but ultimately strategic space for competition, paradoxically exacerbating tensions and instability.

Responding to a cyberattack with a nuclear strike requires absolute certainty as to its true perpetrator. Yet, operations in cyberspace often involve proxies, opaque international relays, and technical masking of the source. An attribution error could have profound consequences. Additionally, a cyber intrusion seen as preparation for a major attack might provoke an overreaction during a crisis. Any doctrine that includes the possibility of a nuclear response must therefore incorporate rigorous *deconfliction mechanisms*, otherwise the worst will happen.

However, these risks should not obscure a strategic reality: current doctrine dates to a time when cyberattacks could not paralyze a country in minutes. This is no longer the case. Adversaries of democratic regimes have understood that cyberspace offers them a means of inflicting considerable damage while remaining below the threshold for a nuclear response. Doing nothing would amount to accepting a structural vulnerability, especially since middle ground is emerging. This involves explicitly defining two categories of cyberattacks likely to trigger an appropriate military response:

1. Attacks causing massive impacts on the civilian population or critical infrastructure (hospitals and emergency services, water distribution networks, etc.).
2. Intrusions targeting the command systems of the armed forces, even without destructive effects, with the aim of degrading a country's decision-making capacity.

Though it would not directly reference nuclear weapons, this clarification would connect strategic cyberattacks to potential responses, giving decision-makers flexibility while clearly warning adversaries. A more explicit doctrine should reduce the risks of accidental escalation and limit the audacity of State and non-State actors willing to test the nerves of democratic regimes, in line with recent analyses on the evolution of the U.S. nuclear posture in the face of new strategic threats that the war in Ukraine has only exacerbated.

About the Author

Gilles A. Paché is a Professor of Marketing and Supply Chain Management at Aix-Marseille University, France, and a member of the CERGAM Lab. His research focuses on logistics strategy, distribution channel management, and military studies. On these topics, he has authored over 700 scholarly publications, including articles, book chapters, and conference papers, as well as 24 academic books. Views expressed in this article are the author's own.