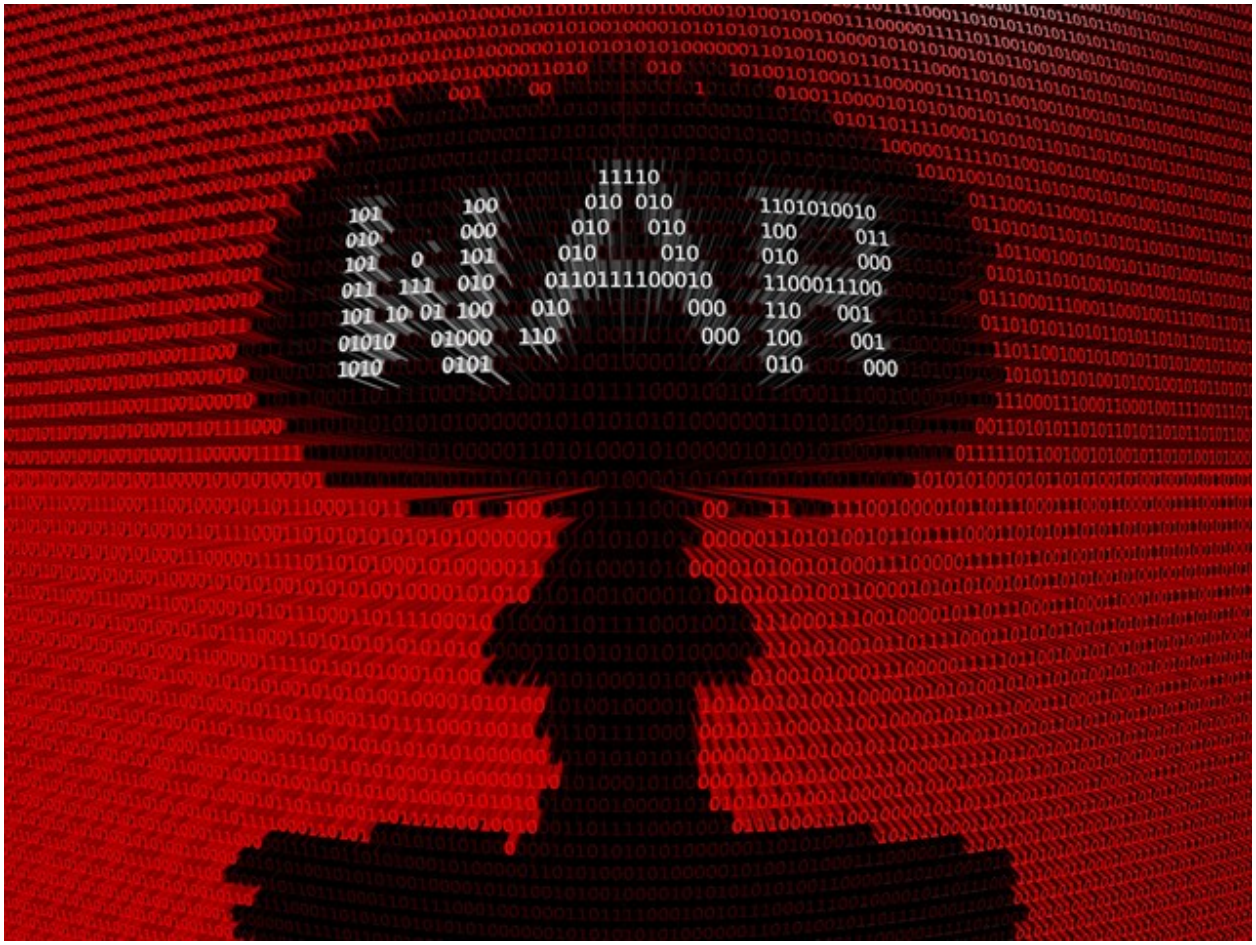
Cyberattacks are on the rise but they could be a necessary evil.



Engineering and Technology

Cyber attacks are increasing.

Ransomware attacks, blackouts, and leaks seem to be slowly revealing the fragility of the global order. Just recently, the DOE recently issued a statement that sophisticated nation-state actors could crash the U.S. power grid. These harrowing threats make a convincing case for shutting off our devices and making survivalist plans, but the reality is much less dramatic. Continued growth of our reliance on technology begs the question, *how much should we worry*?

While there are personal reasons to be afraid of cybersecurity issues, this article will focus on implications for national security. Fortunately, according to some scholars like James Andrew Lewis, a catastrophic war due to cyberattacks is unlikely. In fact, there are three ways cyberattacks may be more conducive to peace in a nuclear world.

1. **It is difficult to confidently attribute attacks to actors.**

   Complexity in software creates enough attribution uncertainty such that no actor could reasonably justify full-scale retaliation. Unlike nuclear weapons, actor ambiguity in cyber strips agents of strategic decision making tools, such as the rational actor model, that enable confident responses. In contrast, for nuclear weapons, Iranian enrichment of uranium is clearly attributable. So, actors like Trump can confidently launch a volley of aggressive sanctions. But, when the actor is uncertain, states have to rely on *generic* analysis instead of *personified* analysis, which makes a strategic response harder to justify.

   Indecision may sound bad, but actor ambiguity can be beneficial because it avoids the fundamental attribution error. Fundamental attribution error suggests people are prone to dispositional analysis which is often incorrect. Thus, when governments attribute state actions to disposition, so-called "confident decision making" can become unnecessarily hostile. In the Iran

example, Kenneth Waltz suggests the U.S. exaggerates dangers of Iranian nukes by painting the Iranian regime as irrational. Waltz points out the government's dispositional error by demonstrating how Iranian nuclear development is a rational response to Israel's middle eastern nuclear monopoly. Unlike Iranian nukes, the ambiguity of who does cyberattacks forces states to use a more cautious approaches that could avoid fundamental attribution error.

2. **It is a useful non-nuclear tool for big states.**

   If so many cyberattacks have happened, why hasn't international law risen to regulate it? Lewis argues that U.S. and Russian cyberattacks are intentional strategic tools for both countries to operate below the level of violence to avoid catastrophe. Thus, "catastrophic cyberattacks" defeat the purpose of using cyber in the first place. If a state really wanted a catastrophic attack, it is more likely cyber would supplement conventional or nuclear warfare but not cause a catastrophe itself. Even the aforementioned DOE statement agrees most nation-state attackers are financially, politically, or technologically motivated.

   State willingness to tolerate smaller attacks reflects Michael Kofman's *stability-instability paradox*: to maintain a more stable balance of nuclear power, states tend to accept conflicts "below the threshold of war." In the

context of blackouts, while cyber-blackouts are recoverable, the alternative is long-lasting conventional decimation of the grid.

Admittedly, Kofman also says that cyber-raiding from Russia could have destabilizing effects. However, he agrees that those raids need staying power. According to Lewis, economic resilience and technological development enable quick recoveries that mitigate "staying." Even in elections, most attacks on U.S. elections have been ineffective or counterproductive.

3. **It is a protection from small-state nuclear proliferation.**

   For some nuclear proliferation scholars, proliferation has not caused a war because proliferators like India and Pakistan are content with the status quo. Despite the irrational depictions of Kim Jong Un, the same could be argued for North Korea. Frank Aum suggests that ransomware attack revenue has been Kim's lifeboat amidst aggressive sanctions. Kim knows North Korea is militarily and economically weaker, so it cannot engage in conventional war. Thus, instead of military force, North Korea resorts to cyber because actor ambiguity reduces the risk of retaliation. Aum contends the U.S. should tolerate cyberattacks to ensure North Korea somewhat willingly works within the status quo instead of literally blowing it up or selling nukes to make money instead. Financial theft, in this instance, certainly feels safer than nuclear proliferation to rogue actors or a hail-mary first strike.

The good in the bad and ugly.

While most people might think cyberattacks are definitely a crime, states chose to tolerate it because it is safer than nuclear wars. The bottom line is that cyberattacks are the best-worst option in a nuclear world.