The Asymmetric Threat Landscape: Adversaries who thwart

Critical infrastructure is being targeted systematically by sophisticated state actors and criminal syndicates operating under advanced strategic doctrines. This document will address the Russian, Chinese, Iranian adversaries and also consider the weather and criminal nexus implications to Critical Infrastructure.

Russian Capabilities: Russia has been intentionally targeting both opponents' and potential supply chain critical infrastructure. This approach has considered many of the traditional laws of warfare inconsequential: hospitals, international underwater cables, and telecommunications infrastructure are all fair game. Russia is not alone with increasing interconnectivity of government and civilian systems, and hacking is not an unused method: Russian cyber threat group Midnight Blizzard (aka "APT29," "UNC2452," and "Cozy Bear") has been conducting cyber espionage under Russia's Foreign Intelligence Service (SVR), targeting governments, defense infrastructure, academic institutions, and non-governmental organizations. Commercial entities are increasingly viewed as legitimate economic proxies in broader geopolitical conflicts.

Chinese Capabilities: China considers economic marginalization to be a legitimate military threat. Chinese military doctrine specifically emphasizes targeting opponents' critical infrastructure to mitigate kinetic conflict. Meanwhile, their national strategy emphasizes a "whole of nation" approach to conflict and has made official their "Military-Civil Fusion". Cyber reconnaissance entities are actively shifting away from industrial espionage or ransomware and have pre-positioned access within western critical infrastructure. The strategic objective is not data theft; it is the establishment of dormant access points to disrupt or paralyze energy, water, and transport sectors during a geopolitical flashpoint. This is done not only through cyber-attacks and hacks, but also through embedded backdoors in innumerable governments' and commercial organizations' systems through active participation in technical projects, providing technical resources, and even sourcing or managing fully functional assets. On top of this, China has a growing space capacity with at least 10 "jamming" satellites and multiple ground-based assets able to impact targeted satellites' communications, in addition to "on-orbit grappling" capabilities of certain satellites.

Iranian Operations: Iranian proxies are already attacking American Critical Infrastructure, as seen with the 2026 Stryker attack, with responsibility claimed by Iranian Proxy Groups. Iranian assets, surrogates, and radicalized extremists, as a whole, have become another threat to consider: while many prior threats have been focused on cyber accesses, radicalized extremists and proxy fighters have become a legitimate concern and identified through the US 2026 Counterterrorism Strategy. First, proxy forces and advanced hacker groups allow adversaries to execute deniable, highly disruptive actions against western infrastructure targets, leveraging radicalized actors or opportunistic criminal networks to exploit unpatched edge devices. Second, planting improvised explosive devices or the use of kamikaze drones is an increasingly legitimate threat. Third, some of these proxies may impact US Critical Infrastructure as a secondary or tertiary effect: the Houthis have been purported to sever underseas communication cables in the Red Sea, impacting international communications, and other means of sabotage are not unreasonable or unlikely. CISA has highlighted that Iran is actively using its assets to target the following: (1) opportunistic disruptions, (2) cyber espionage to inform kinetic strikes or assess battle damage, (3) pre-positioning and foot-hold establishment for later use, and (4) cyber-enabled information operations – like hacking electric signs.

Weather: Weather deserves to be highlighted not simply for compounding attacks, but also the everyday effects. Water and heat are both impacting operations and compounding challenges: areas like Corpus Christi port area and the California with her Data Centers are threatened with severe water shortages, challenges from Wild Fires impact operations and supply chain sustainability, drought is compounding impacts to agriculture (from worker, fuel, and fertilizer shortages), and freezing temperatures are known to stop the flow of goods or energy.

Criminal Syndicates and State Proxies: Financially motivated cybercrime and state-sponsored gray-zone operations do not exist in silos. The contemporary threat landscape is characterized by a dangerous convergence where transnational criminal organizations (TCOs) and illicit financial networks are actively weaponized as state proxies to exploit critical infrastructure vulnerabilities.

- **The Crime-Terror Convergence:** The established, multi-decade operational integration between Iranian proxies like Hezbollah and Latin American drug cartels serves as a primary case study for this threat nexus. These syndicates no longer operate merely for localized profit; they function as logistical force multipliers for hostile nation-states.

- **Asymmetric Vectors of Entry:** By leveraging the sophisticated smuggling routes, illicit financial laundering mechanisms, and corrupted supply chains controlled by criminal cartels, state adversaries can bypass traditional border and cyber defenses. This allows hostile actors to insert physical payloads, deploy insider threats, or establish localized operational footholds within Western territory.

- **Plausible Deniability in Hybrid Warfare:** This symbiotic relationship grants state sponsors total plausible deniability. A seemingly isolated cyber disruption, ransomware extortion event, or physical sabotage incident at a critical infrastructure hub can be executed via a criminal cutout, masking a targeted geopolitical strike as a routine act of corporate extortion or localized criminality.

Consequently, criminal networks are not peripheral law enforcement concerns: they are active, heavily subsidized vectors of state-directed hybrid warfare capable of striking through highly unconventional avenues.