

Cyber Deterrence Begins with the Power to Disconnect

By
Burak Oktenli

Published: 20 October 2026

On August 26, President Donald Trump declared a national emergency over foreign actors exploiting vulnerabilities in the U.S. bulk-power system. The order framed the problem as one of national security, public safety, and economic resilience. A month later, [CISA issued new guidance on cyber decoys](#) to help critical-infrastructure defenders catch intruders using legitimate credentials and native tools. Those moves improve prevention and detection. They do not answer the harder deterrence question: what happens after defenders discover that a sophisticated adversary is already inside?

If removing hostile access would also halt power, logistics, communications, or another essential service, the intrusion can create leverage before a destructive command is ever issued. The strategic problem is therefore larger than penetration. It is whether the defender can withdraw trust without inflicting the disruption the adversary hoped to create.

A Foothold Can Coerce Without Firing

The U.S. has already documented the pre-positioning problem. A joint federal fact sheet on [Volt Typhoon](#) says the People's Republic of China-linked group compromised organizations in communications, energy, transportation, and water systems to position itself for potential disruption during a future crisis. Pre-positioning matters because an unused foothold can still shape decisions if leaders believe evicting it will damage their own mission.

This is a form of coercive dependence. A defender can become so reliant on a remote connection, cloud service, supplier, identity system, or shared data source that severing the compromised path appears nearly as costly as leaving it in place. An adversary then gains value from access even without activating a destructive effect.

Selective Disconnection Is Deterrence by Denial

Joint [CI Fortify guidance released in July](#) addresses the operational side of this problem. It urges critical-infrastructure operators to prepare to isolate vital operational technology and enabling systems while maintaining essential operations. Britain's [operational-technology guidance](#) likewise distinguishes full site isolation from service-specific isolation and hardware-enforced trusted communications.

The strategic value is in the word selective. A suspected component may still be allowed to observe while losing permission to issue commands, change configurations, move resources, or communicate outside a defined boundary. The goal is to remove the adversary's options faster than the defender removes its own mission.

This is deterrence by denial at the level of system architecture. An attacker that expects access to produce a reliable ability to stop the mission gains less from the intrusion if the defender can rapidly reduce that access to a narrow, monitored state while essential functions continue.

The Disconnect Control Can Be Attacked Too

Isolation is not automatically safe. False alarms, manipulated telemetry, or ambiguous indicators can push defenders toward unnecessary shutdowns and hand an adversary disruption without a successful destructive action. Exercises should therefore evaluate both genuine compromise and misleading evidence, including who can impose restrictions, which facts justify the decision, and how an incorrect restriction is reversed.

The same discipline applies to the control plane itself. The authority to isolate a site, revoke a supplier, or cut a management path should not depend on the same compromised credential or platform it is meant to constrain. Separation of duties and independent control paths turn disconnection from a policy promise into an operational capability.

Recovery Must Be Earned

Disconnection is only half of the problem. A defender that can isolate a compromised dependency but cannot establish when reconnection is justified may trade adversary leverage for self-imposed paralysis. [NIST's cyber-resiliency engineering guidance](#) defines resilience around the ability to anticipate, withstand, recover from, and adapt to attacks or compromise while reducing mission risk from dependence on cyber resources.

Recovery should therefore be configuration-specific and evidence-based. Restoring connectivity does not prove that credentials, software, data, and control paths are trustworthy again. Decisionmakers should know which configuration is returning, what evidence supports renewed trust, what limitations remain, and who accepts the residual risk.

Measure the Denial Capability

Three measures can turn these concepts into a deterrence capability that leaders can evaluate. The first is containment time: how quickly can the defender restrict the suspected dependency? The second is mission effect preserved during isolation: what essential service remains available? The third is trusted recovery time: how long before access and authority can be restored on a defensible evidentiary basis?

These measures matter across alliances as well as inside a single operator. President Trump's June [national cybersecurity memorandum](#) calls for key military and intelligence missions to remain viable in contested cyber environments and for greater coordination across agencies, industry, and international partners. Shared cloud services, communications, logistics systems, and identity providers make one partner's isolation decision capable of affecting another partner's readiness.

No serious cyber strategy can promise that capable adversaries will never penetrate important systems. The stronger deterrence signal is that penetration does not guarantee strategic leverage. A defender that can detect a foothold, sever the dangerous dependency without surrendering its essential mission, and restore trust for evidence makes access less valuable in the first place.

A decoy can reveal that an adversary is inside. Deterrence begins when the defender can take that access away without taking itself offline.

Burak Oktenli is an independent researcher based in Washington, DC, conducting research on deterrence, cyber resilience, assurance, and machine authority in autonomous systems. His analysis has appeared in Global Security Review, RealClearDefense, the Modern War Institute at West Point, RUSI, and Articles of War. Views expressed in this article are the author's own.