THE CYBER DEFENSE REVIEW
2026, VOL. 11, NO. 2, 221-227
https://doi.org/10.55682/cdr/y0f7-s7pf

SENIOR LEADER PERSPECTIVE

China's Cyber Explosives are in Place. Where's our Response?

Rob Joyce

Joyce Cyber LLC, MD, USA

Drawing on recent cyber intrusions into U.S. critical infrastructure, Rob Joyce, former Acting Homeland Security Adviser on the U.S. National Security Council and retired NSA Director of Cybersecurity, argues that the People's Republic of China's campaigns—such as Volt Typhoon and Salt Typhoon—are not routine espionage, but deliberate preparations for conflict. These operations reflect a coordinated effort to pre-position access across vital systems, enabling the potential disruption of military logistics and civilian infrastructure in the early stages of a crisis. The article contends that U.S. deterrence has failed not for lack of capability, but for lack of resolve and strategic coherence. Cyber operations exploit a critical asymmetry: their effects are often invisible, deniable, and insufficient to trigger decisive political action. As a result, adversaries have been able to operate below the threshold of response while steadily expanding their foothold. The temporary decline in activity following the 2015 U.S.–China cyber agreement demonstrates that deterrence is achievable—but only when costs are imposed visibly and across domains, particularly through economic and diplomatic leverage. The piece concludes by calling for a whole-of-government approach that treats cyber intrusions into critical infrastructure as intolerable national security threats. It emphasizes the need for visible, coordinated responses—led at the presidential level—to restore credible deterrence and prevent adversaries from exploiting persistent access within U.S. systems.

Keywords: cyber deterrence, critical infrastructure security, state-sponsored cyber operations, China cyber strategy, pre-positioning attacks, cross-domain deterrence

Rob Joyce served over 34 years at the NSA in multiple roles. Rob finished his career as the Head of the Agency's Cybersecurity Directorate. He also served on the White House National Security Council as a Special Assistant to the President and Cybersecurity Coordinator, as well as Acting Homeland Security Advisor. Throughout his career, Rob led operations pursuing the most sophisticated hackers and innovated technologies to protect vital national assets—including US classified networks and nuclear authorization codes. He is now the Founder of Joyce Cyber LLC and serves on boards and in advisory capacities, utilizing his cybersecurity expertise. He is a frequent speaker, talking about cyberthreat, artificial intelligence, and cyber policy.

America's critical infrastructure is under siege, yet we treat cyberwar as a technical problem rather than a national security crisis.

We've reached a chilling milestone: China has effectively strapped the digital equivalent of explosives to the backbone of American society. Imagine if we discovered physical bombs attached to our power plants, pipelines, or water systems. Our response would be immediate and overwhelming. Yet because the threat exists in cyberspace, we've done almost nothing. We've treated it as a manageable nuisance rather than an act of war.

The cybersecurity metrics tell a sobering story. Over the past decade, cyber intrusions have exploded in frequency and severity. Each year seems to set new records for hacks and associated damage; the FBI (2024b) IC3 Annual Report noted they received 859,532 complaints in 2024 , the most ever, and the 2025 stats are not yet in. Dragos (2026) identified 3,318 industrial organizations impacted/victimized in 2025. But statistics alone don't capture the peril of what's now occurring. While we've been fortifying our digital networks, our adversaries have been honing their exploitation capabilities with even greater success. Cyber used to be about espionage and commercial theft. It was serious, but it was bounded. That era is over. Cyber operations are now a feature of every geopolitical conflict and a continuous background activity even outside declared hostilities. Nations are using cyber to shape, coerce, and prepare the battlefield in peacetime. The most consequential shift: critical infrastructure is in the crosshairs. Chinese hackers have systematically infiltrated America's most vital systems, including our electric grid, water treatment plants, transportation networks, pipelines, and telecommunications infrastructure. Quietly maintaining access. Waiting.

The PRC has hacked its way into our most vital networks. They have the access they need and are ready to deliver devastating effects from China at the time of their choosing, throwing the country into chaos. A joint advisory from CISA and NSA (2024) warned that these intruders aren't just stealing data; they are "pre-positioning themselves" to disrupt or destroy systems in a crisis. Despite our cyber defenses improving year after year, we are losing the cyber fight and losing badly.

THE TARGETING WAS NOT RANDOM

The pattern of Chinese infiltration tells us something important that we have largely failed to say out loud: this is not espionage. This is war preparation with a specific target date in mind.

Volt Typhoon, the Chinese state-sponsored campaign that became the public discussion of U.S. intelligence in 2023, did not waste effort burrowing into agricultural supply chains or entertainment platforms. The People's Liberation Army Strategic Support Force went for transportation command centers, West Coast port logistics, Guam communications infrastructure, and the fiber interconnects that would carry military orders in a Pacific crisis. That pattern of infiltration is itself an intelligence product. It tells us exactly what Beijing believes it would need to paralyze in a Taiwan contingency, and it tells us that China has already run the operational calculus on which systems to disable and in what sequence.

This is not pre-positioning for leverage in routine geopolitical competition. This is a military operation conducted in peacetime, on American soil, inside American infrastructure, targeting the specific nodes that would be critical in the first 72 hours of a shooting war across the Taiwan Strait. We should be calling it what it is. The fact that we haven't says more about our political will than our analytic capabilities.

Think concretely about what coordinated activation of those implants looks like. Darkened ports on the West Coast unable to move military cargo. Communications disruptions to Pacific Command at the precise moment operational orders need to flow. Pipeline pressure anomalies requiring manual shutdown in multiple states, diverting first responders away from military logistics. None of these are hypothetical; they are the operational logic embedded in the targeting choices Beijing has already made. The explosives aren't placed randomly. They are placed for a specific detonation scenario.

Worse than military impact, these operations are also intended for domestic terrorism within the US. In April 2024, then FBI Director Christopher Wray said "The PRC has made it clear that it considers every sector that makes our society run as fair game in its bid to dominate on the world stage, and that its plan is to land low blows against civilian infrastructure to try to induce panic and break America's will to resist." (FBI 2024a) Inducing panic… They want to terrorize our population.

WHY DETERRENCE HAS FAILED

Our lack of deterrence represents a fundamental failure of imagination and resolve across multiple administrations. While not every hack is an act of war, those that endanger lives or critical services cross a line warranting a forceful response. We've allowed our adversaries to position themselves for devastating attacks while responding with piecemeal efforts and weak responses.

There are growing calls for more aggressive offensive cyber operations to deter these intrusions. While credible cyber response actions are needed, they are only part of the solution. Offensive cyber operations alone don't deter cyber operations; they escalate them. When we discovered Chinese hackers embedded in our critical infrastructure, it didn't make us step back. It raised more calls to hack their networks. This tit-for-tat dynamic only ensures mutual vulnerability without addressing the core problem.

It's worth asking why cyber deterrence has proven so structurally resistant to the lessons of other strategic domains. Nuclear deterrence worked because consequences were undeniable, irreversible, and publicly visible. A mushroom cloud over a city is not subject to attribution debates. Cyber effects, by contrast, are often reversible, plausibly deniable, and invisible to the public. Populations that don't know they've been attacked don't generate the political pressure needed to sustain a response. Beijing

has exploited that asymmetry brilliantly. They operate in the gap between what our intelligence community can see and what our political system can act on.

The answer is not to accept that gap. It is to close it by making our responses visible even when attacks are not. Attribute aggressively and publicly, but then use the real elements of our national power: Diplomatic, Information, Military, and Economic tools with real teeth. Make Beijing pay costs that are legible to their own public and to international partners, not just costs visible in classified cable traffic that never reaches a newspaper.

THE ONE TIME IT WORKED

The one moment we saw China pause cyber operations came after 2013 President Obama made intellectual property theft a personal issue with President Xi Jinping and commitments were reached in 2015. The message was clear: continue this behavior and face broader consequences. There was a noticeable drop off of cyber operations for a period after the President made legitimate threats of cost imposition. In 2017, Kevin Mandia provided testimony to the Senate Intelligence Committee stating: FireEye "saw a sharp decline in these operations after September 2015," referring to the period after Obama and Xi met and made their cyber commitments (Mandia 2017). Since then, we've lost that clarity of communication and strong demonstration of resolve.

That moment deserves more careful analysis than it typically receives. It wasn't simply a private conversation between presidents that produced the pause. The mechanism was specific: Obama credibly threatened to tie Chinese cyber behavior to trade relationships, and Xi understood that the economic consequences would be real and public. It was not a cyber response to a cyber attack. It was a cross-domain response, one that used economic leverage where China was genuinely exposed. The lesson from 2013 is that deterrence requires credible costs in domains where the adversary cannot absorb them. Beijing can absorb our cyber counter-operations. They cannot absorb, without serious consequence, targeted economic pressure applied at scale and sustained by a coalition of allies. This lesson isn't about financial costs, it's about finding levers of pain that convince an adversary we are deadly serious.

We've forgotten that lesson. Worse, we've allowed administrations to treat each Chinese cyber campaign as an isolated incident rather than a pattern of behavior warranting a cumulative response. Every time we reset the deterrence clock, Beijing's calculus becomes clearer: the Americans will complain, indict some PLA officers who will never face trial, issue a strongly worded statement, and move on. We have trained them to believe the cost of intrusion is essentially zero.

WHEN THE ACTUARIES CROSSED THE LINE BEFORE THE SITUATION ROOM DID

In 2022 and 2023, Lloyd's of London and other major insurers moved to exclude nation-state cyber-attacks from standard commercial policies. Insurance underwriters, whose entire business model depends on accurate risk pricing, had concluded what our policy community still refuses to state plainly: these are not commercial risks. They are acts of warfare, too catastrophic and too correlated to be insurable under normal terms.

We should be embarrassed that the actuarial tables made that determination before the Situation Room did. The insurance industry has no political incentive to declare war. They did it because the

math forced them to. The math is the same math available to our policymakers. The difference is that Lloyds acts on it, and Washington doesn't.

The practical consequence of that exclusion matters beyond the policy debate. Critical infrastructure operators who thought they had financial backstop against catastrophic cyber events now do not. The private sector owners of our most vulnerable systems, the power companies, the pipeline operators, the port authorities, are now carrying tail risk they cannot price and cannot hedge. That is not a business problem. It is a national security problem that manifests on the balance sheets of private companies. And it is a direct consequence of the federal government's failure to deter the threat in the first place.

SALT TYPHOON AND THE INSTITUTIONAL SELF-SABOTAGE

Consider the notable lack of response to recent revelations that Chinese hackers penetrated America's largest telecommunications companies, allegedly compromising information from presidential candidate Trump and vice-presidential candidate Vance (Tucker, Balsamo, and Miller 2024). Some in Congress called the Salt Typhoon incident "the most damaging breach of America's phone system in recent memory" (Vicens and Setter 2025). Neither the outgoing nor incoming administration mounted a major presidential-level response.

The Department of Homeland Security then canceled its planned retrospective study of the Salt Typhoon breaches. That decision deserves far more attention than it received, as we have no authoritative learnings from our failures against this PRC intrusion.

When the government cancels its own after-action review of the worst telecommunications breach in American history, it doesn't just send a signal to Beijing. It ensures that the institutional lessons that would inform the next response are never captured, never disseminated, and never acted upon. The next administration inherits the vulnerability without the analysis. The cycle repeats. Beijing watches and concludes that American institutional memory is as brittle as American political will.

The telecommunications companies whose networks were compromised had been warned for years about the vulnerability of legacy protocols. The Salt Typhoon breach wasn't a bolt from the blue. It was a slow-motion failure of regulatory accountability and corporate risk tolerance. The telecom executives made a rational business decision: compliance with enhanced security standards costs money and the regulatory consequences of non-compliance cost less. We built that incentive structure. It produced the breach. Canceling the after-action review ensures we learn nothing that might require us to change it.

THE COALITION WE BUILT AND THEN ABANDONED

The 2021 attribution of the Microsoft Exchange hack, co-signed by more than 30 nations, represented something historically unprecedented in international cyber politics: collective attribution with collective pressure. Thirty nations stood together and named China publicly, with coordination that had never been achieved before at that scale.

For Volt Typhoon and Salt Typhoon, incidents of far greater strategic consequence to American security, no comparable coalition response materialized. The explanation is not a failure of diplomacy.

It is that our allies watched us cancel our own after-action review of Salt Typhoon and drew the obvious conclusion about American resolve. You cannot lead a coalition from a posture of strategic ambivalence.

The allied dimension matters for a reason beyond coalition optics. Several of our Five Eyes partners and our key Indo-Pacific allies, Japan and Singapore in particular, have similar exposure to Chinese infrastructure penetration and similar incentives to act. But they are also more economically dependent on Chinese trade relationships than we are willing to acknowledge on their behalf. Effective deterrence requires that we be willing to absorb some of the economic cost of allied solidarity, to make clear that the United States will not leave partners exposed when they stand with us in attributing Chinese aggression. We have not made that commitment credibly. Until we do, we will continue to lead coalitions that dissolve the moment Beijing applies economic counter-pressure.

THEIR TIMELINE AGAINST OUR CALENDAR

Xi Jinping operates on a 25-year strategic horizon. American presidents get four-year windows and change national security staff wholesale at transitions. One house of congress faces reelection every 2 years. Those are not strategic timeline horizons. The cancellation of the Salt Typhoon retrospective captures that mismatch in miniature: incoming administrations don't want to own the failures of their predecessors, so they bury the record rather than learn from it. The institutional knowledge that would produce a sustained, coherent deterrence strategy gets discarded with each change in administration, while the PLA's access to our infrastructure compounds year over year.

This structural disadvantage is not insurmountable, but overcoming it requires deliberate institutional design: independent oversight bodies with continuity across administrations, statutory requirements for incident reporting and after-action analysis that no administration can simply cancel, and cyber policy commitments embedded in treaty structures that survive election cycles. These are not small asks in a polarized political environment. They are the minimum requirements for a deterrence posture that Beijing will actually credit.

A NEW APPROACH

The U.S. still has options to turn the tide. We need a new approach that treats cyber intrusions into critical infrastructure as the intolerable acts they truly are. Offensive cyber responses won't change the game. This doesn't mean we should abandon offensive cyber capabilities. Offensive cyber operations remain an important tool in our responses. But they must be part of a comprehensive strategy that employs all elements of national power: diplomatic pressure, economic sanctions, intelligence operations, and the credible threat of traditional military action.

For example, our response to an intrusion could include publicly naming and indicting the culprits, expelling diplomats within 48 hours of discovery, sanctioning tech imports, conducting counter-cyber operations, initiating sanctions, all paired with diplomatic ultimatums from the White House. Coordinated and powerful actions with unambiguous leadership messaging is vital. The President. The tools exist. The question is whether we'll use them.

Adversary leaders must believe that the costs of their cyber intrusions will outweigh any benefits. This requires presidential-level attention and clear communication that certain lines, once crossed,

will trigger escalatory responses across multiple domains. It means making cyber attacks on critical infrastructure as unthinkable as physical attacks on the same targets.

THE DECISION POINT

There is a communication failure embedded in this crisis that leaders rarely acknowledge. When U.S. intelligence declassified the Volt Typhoon warnings in early 2024, public response was muted. That is partly because the government disclosed the threat without translating it into human consequence. The American public authorized massive industrial mobilization in 1941 because they understood viscerally what Pearl Harbor meant. Leaders who cannot translate cyber risk into human consequence do not get the public mandate they need to act. That is a leadership failure, not a technical one.

The digital intrusions will continue until we decide that enough is enough. America can no longer afford to have its leaders silo cyberattacks as an IT problem separate from geopolitics. We'll know we've reached that decision point when the president is personally engaged in responding to these attacks, when we're marshaling diplomatic pressure alongside technical defenses, when we use all elements of national power and when our adversaries genuinely fear the consequences of their actions.

Until we change our policy, we're simply allowing China to complete its preparations inside our infrastructure. In cyber as in the physical world, aggression unanswered is aggression encouraged. They are engaged in a conflict we seem determined to pretend isn't already underway. The digital explosives are in place. The question is whether we'll act before detonation.

REFERENCES

Dragos. 2026. *OT Cybersecurity Report: Adversaries Increase Real-World Impact, Map Control Loops Across Industrial Infrastructure.* Dragos, February 17, 2026. https://www.dragos.com/resources/press-release/dragos-2026-year-in-review-new-ot-threats-ransomware.

FBI (Federal Bureau of Investigation). 2024a. "Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says," April 18, 2024. https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says.

FBI (Federal Bureau of Investigation). 2024b. *Internet Crime Report 2024.* Internet Crime Complaint Center (IC3). https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

Mandia, Kevin. 2017. *Prepared Statement of Kevin Mandia, CEO of FireEye, Inc. before the United States Senate Select Committee on Intelligence.* United States Senate Select Committee on Intelligence, March 30, 2017. https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-os-kmandia-033017.pdf.

NSA (National Security Agency). 2024. "NSA and Partners Spotlight People's Republic of China Targeting of U.S. Critical Infrastructure," February 7, 2024. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3669141/nsa-and-partners-spotlight-peoples-republic-of-china-targeting-of-us-critical-i/.

Tucker, Eric, Michael Balsamo, and Zeke Miller. 2024. "Chinese hackers targeted phones of Trump, Vance, people associated with Harris campaign." *AP News* (October 25, 2024). https://apnews.com/article/china-fbi-trump-vance-hack-cellphones-d085787db764d46922a944b50e239e4a.

Vicens, A.J., and Raphael Setter. 2025. "US DHS fires outside advisers, sources say China probe disrupted." *Reuters* (January 21, 2025). https://www.reuters.com/world/us/us-department-homeland-security-firing-all-advisory-committee-members-letter-2025-01-21/.