TA Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Glenn Chafetz

How can the US protect its health infrastructure against Russian and Chinese cyberattacks?

The attack by the Russian ransomware group ALPHV BlackCat on Change Healthcare on February 21, 2024, delayed treatment for untold numbers of patients and threatened the solvency of thousands of hospitals.

In early 2020, at the outset of the COVID-19 pandemic, China ramped up imports and restricted exports of personal protective equipment (PPE), exacerbating shortages and driving up prices in the United States.

These are two well-known examples of how the US health care system is dangerously vulnerable to disruption by the governments of Russia and China and their proxies.

This vulnerability is multifaceted, coming directly via cyber attacks, control of medical supply chains, and data theft, as well as less directly via infiltration of other infrastructure upon which medical care depends, including telecom, energy, transportation, and power.

These attacks produce at least three types of harm: they disrupt treatment to patients, they damage the US economy; and they provide US adversaries with critical data they can exploit for further attacks.

The attackers

China and Russia are not alone among cyber threats to the United States; Iran and North Korea also maintain programs for attacking US infrastructure, including hospitals, but Russia and China operate at a much greater scale.

Predictably, Russia and China publicly deny any responsibility for any infrastructure breaches.

Even when they acknowledge that an incident occurred, the two governments ascribe responsibility to unknown actors, or at most, criminal gangs beyond governmental control.

> Russia relies on a mix of state and private actors to implement its cyber attacks

These denials are not credible, and the US government has rejected such claims by both China and Russia.

Both governments are totalitarian dictatorships, and the so-called non-state actors responsible for attacks on the United States work at the direction of, or in some cases, the tolerance of their governments.

In China, the iSoon leaks conclusively reveal the network of companies and contracted groups pursuing cyber operations against the United States at the behest of the Chinese Communist Party (CCP).

Russia similarly relies on a mix of state and private actors to implement its cyber attacks.

Supply disruption

The United States depends on Chinese manufacturers for a vast array of products necessary for the function of the US healthcare system. PPE is the most obvious, owing to the pandemic.

Although a number of US companies entered the PPE market during the pandemic, most of those companies cannot compete with Chinese producers on price.

Therefore, China remains the dominant supplier of PPE, and the United States remains just as vulnerable to Chinese government restrictions on PPE imports and exports.

China also dominates the supply of other critical items such as syringes, needles, tubing, gauze, and catheters.

While these items seem simple to manufacture, the United States does not make nearly enough of them, and it is impossible to deliver care to patients without them. Thus, a disruption in their supply would be catastrophic.

Pharmaceuticals are another area of significant US dependence on China. Direct imports of active pharmaceutical ingredients

(APIs) from China are close to 17 percent, (higher estimates of 80 to 90 percent are based on a faulty interpretation of data), but indirectly China's importance to the US market is much greater.

> The United States currently imports under three percent of total purchases of these products from China

US drug companies obtain the supplies for their products from 47 different countries, and China is the number one exporter of APIs worldwide.

For an example of indirect influence, China supplies 70 percent of India's APIs, and India is one of the largest suppliers of pharmaceuticals to the United States.

Just as important as how much the United States and other countries have outsourced to China is what they have outsourced: the most dangerous chemical reactions, using the most toxic chemicals in the synthesis of key starting materials.

This is important because few companies in the United States want to do this work.

Another category to watch is higher-end medical supplies, including devices, therapeutics and diagnostics (e.g. stents, ventilators, surgical instruments, diagnostic machinery).

However, while China produces and exports a growing share of these items at a more competitive price, the United States currently imports under three percent of total purchases of these products from China.

Direct cyber attacks on healthcare infrastructure

According to the Wall Street Journal, among various economic sectors, healthcare may be uniquely vulnerable to cyber attacks: hospitals and physicians' offices underinvest in technology and training; keep too much data and face no regulatory consequences for associated HIPAA violations; and readily pay ransomware so as to avoid lapses in care.

Russia is the principal source of direct cyber assaults on hospitals, physicians, insurance companies, and other health infrastructure.

Most of its attacks involve ransomware. The 2024 Change Healthcare ransomware attack was the single most damaging of such events in history, affecting more than 100 million patients.

Interruptions in computer network functions in hospitals mean interruptions to the full range of care, including distribution of medications, discharges and admissions, blood draws, scheduling, and communication for staff and patients.

Hospitals and other care facilities are ill-equipped to deal with these attacks. A 2024 survey showed that total annual spending on information technology (IT) averaged three percent of total spending.

The 2024 Change Healthcare ransomware attack was the single most damaging of such events in history, affecting more than 100 million patients

Another survey revealed that spending on cyber security averaged less than 10 percent of hospital IT budgets – or under .3 percent of total spending.

Furthermore, some respondents did not know how much they spent, and others complained that they did not have the funds to recruit the most in-demand cybersecurity professionals.

Emergency room physician, Dr. Michael Lynn, told the author that hospitals need to not only invest more in security but also in plans for continuity of operations when security fails:

"The key is actually to focus on how to stay open when a ransomware attack occurs, not focus solely on prevention, because ultimately it's going to happen. To stay open for critical functions means creating a tiered approach where the most critical services are isolated from the rest of the hospital; the ER, OR, pharmacy, laboratory, CT scan, anesthesia, certain devices such as IV pumps, etc. This would be Tier 1 (which also relies on water and power, a related challenge). As long as Tier 1 is protected, the hospital stays open and panic is minimized."

China has not yet been implicated in a direct cyber attack on the US healthcare system, but the US government and the American Hospital Association are worried that such attacks are just a matter of time.

This is because Chinese-manufactured medical devices are so common throughout the US healthcare system, because those devices are increasingly networked and thus vulnerable to exploitation, and because China has a history of exploiting backdoors in the products it manufactures.

The FDA was so concerned about this in June 2025, it issued mandatory guidance on the cybersecurity standards of networked devices.

Indirect infrastructure attacks affecting hospitals

Even the best preparation for a ransomware attack on a hospital will not keep it open in the event of a large-scale attack on power, energy, water, communications, finance, or transportation infrastructure.

Any degradation in those systems will necessarily reduce the ability of hospitals to function.

Both Russia and China have incorporated infrastructure attacks in their ongoing covert operations against the United States.

> Russia and China were responsible for cyber compromises of US communications, energy, transportation systems, and water and wastewater systems

The US government has concluded that Russia and China were responsible for cyber compromises of US communications, energy, transportation systems, and water and wastewater systems.

Examples abound: in 2009, both Russia and China penetrated the US power grid; in 2010, Russian actors planted a "cyber grenade" in the NASDAQ stock exchange; in 2018, the US Department of Justice indicted four Russians tied to the Ministry of Defense with hacking into the Wolfcreek nuclear power plant in Kansas; and in 2021, Chinese hackers breached the New York City Metropolitan Transit Authority system that controls the subway.

Theft of data and intellectual property

Attacks on healthcare infrastructure can involve theft as well as destruction of function. (Ransomware notoriously includes both, as it relies on destruction as a means to steal the target's funds via extortion.)

Chinese actors are more known for theft of data and intellectual property (IP), including drug characteristics and the results of clinical trials, while Russian groups are behind the vast majority of ransomware. Data theft is usually a means to an end.

In addition to IP theft (commercial espionage), Chinese groups steal the personal data of Americans to learn about and exploit their financial and health vulnerabilities.

The most famous example of patient data theft attributed to China is likely the Anthem insurance company hack of 2015

Chinese intelligence services use this information to target specific individuals for espionage, influence, and IP theft.

Patient data can be used for all those purposes, as well as to advance China's biotech industry and even to extend the CCP's ubiquitous domestic surveillance to the United States.

The most famous example of patient data theft attributed to China is likely the Anthem insurance company hack of 2015, which compromised data on 78 million Americans.

Misaligned incentives

If Russia and China used physical explosives instead of malware against US hospitals, the US government would react much more immediately, harshly, and likely violently.

However, while espionage and sabotage are less visible and dramatic than bombs and bullets, they are no less damaging, having caused some number of premature deaths; delayed care and loss of privacy for millions; costs in the hundreds of billions of dollars in lost revenues, ransomware payments, downtime in operations, and recovery efforts; and incalculable damage to US national security.

According to one study from 2020, drug piracy alone costs US pharmaceutical companies between 37 and 162 billion dollars per year in lost revenue, and piracy is just one vector of harm to the overall US healthcare system.

Hospitals need to improve their prevention, detection, communication, reporting, and incident response under various scenarios

Healthcare accounts for almost a fifth of US GDP, and yet neither the government nor the healthcare establishment has a coherent strategy for defending the various components of this critical sector.

As noted above, spending on securing systems and data is insufficient. Hospitals need to improve their prevention, detection, communication, reporting, and incident response under various scenarios.

Moreover, few hospitals and other providers have plans for continuity of operations in the event of a loss of function or interruption of critical equipment and supplies.

This responsibility for a stronger defense is not limited to the healthcare industry. The US government needs to provide stronger support to this critical sector; known US government reactions to the most egregious attacks like those on Change and Anthem were tepid.

Healthcare institutions must defend themselves

China and Russia pay no price for the war they wage, and so they continue to wage it. Big tech also shares responsibility for the endemic vulnerability of American healthcare to predation.

US software developers continue to put out products in which security is an afterthought at best, as the July 2025 Microsoft software vulnerabilities and compromises demonstrated.

Sadly, these breaches will continue because big tech lacks any incentive to improve the security of its products. It faces no fines or other disincentives to alter business as usual.

Few hospitals and other healthcare organizations correctly assess the probabilities of losses, in part because of weaknesses in detection and underreporting of attacks.

Moreover, attacks and losses, even when reported, are diffused among tens of thousands of organizations.

Underreporting means that individual executives underestimate the overall probability of attacks.

Diffusion means those same executives believe attacks happen to others and not their own organizations.

As a result, healthcare organizations spend less time and money than they should on security.

To the degree that they do, they focus on IT and HIPAA compliance and ignore human-centric threats found in hiring, contracting, procurement, and information sharing practices.

Few healthcare institutions train employees in threat recognition. Without knowledge of the threat actors and their techniques, allocation of resources for threat mitigation is impossible.

While Russia constitutes a significant malware threat and deserves attention, it pales in comparison to the damage that China inflicts on the US healthcare system and supporting infrastructure.

China dedicates and coordinates the resources of its entire, massive state-party-intelligence apparatus, to cripple US healthcare and other critical infrastructure in the event of a hot war

Thus, the bulk of security dollars should go toward preventing and mitigating the various attack vectors the Chinese government and its proxies employ.

The CCP views itself in a cold war with the United States. China dedicates and coordinates the resources of its entire, massive state-party-intelligence apparatus, with its prodigious economic and scientific capabilities, to cripple US healthcare and other critical infrastructure in the event of a hot war.

Beijing regards the conflict as existential; as long as the current cold war continues, the CCP will continue to bleed the US healthcare system of its intellectual property, patient data, and dollars, with the ultimate goal of rendering the United States economically and politically irrelevant.

The US government can certainly do more, including by disincentivizing US investment in drug development and manufacture and imposing higher costs for Russian and Chinese attacks on the US healthcare system.

However, the federal government lacks the authorities and resources required to defend every hospital, insurance company, physician's office and all their supporting elements of technology, infrastructure, and supply chain against every attempted cyber intrusion, ransomware event, insider threat, data breach, and theft of IP.

The attack surface is too big and lucrative a target, and the governmental assets for defending that target (FBI, Homeland Security, etc.) are too small, insufficiently resourced, task-saturated, and legally constrained to be effective.

Healthcare institutions, together with other critical infrastructure and big tech, must defend themselves. No one is coming to their rescue, and the problem is not going away.

Glenn Chafetz is the Director of 2430 Group, a

non-profit, non-partisan institution that produces and disseminates research on state-sponsored espionage against the U.S. private sector. Glenn has more than 30 years of experience in government, academia, and the private sector. He spent most of his career at the CIA, where he served multiple overseas tours, including three as Chief of Station. He was also the Agency's first Chief of Tradecraft and Operational Technology.