Facing 21st-Century Threats: What Every Consequence Manager Should Know

Background

Because of evolutions in technology and traditional military production, the United States is facing a rapidly evolving threat landscape—one very different from the landscape it faced just 25 years ago. More adversaries have gained the ability to inflict harm on the homeland, and the US must contend with increases both in the number of potential targets it must defend and in the variety of methods it must defend against. To meet this challenge, consequence managers need to prepare for unprecedented consequence management missions.

The first step in preparing for these missions is to consider three key questions:

- Which threat actors have the intent and ability to harm the US?
- What are their most likely and most impactful targets?
- What vectors will they use to attack?

For the United States, the threat **actors**, likely **targets**, and **vectors** are known, as described in the next section.

Threat actors

The most significant state-based threats to the US come in two groups of states: the regional powers Iran and North Korea, and the global powers Russia and China.[1] Foreign terrorist organizations continue to develop their ability to target US assets abroad and in the homeland, but this product is focused on the more emergent threat posed by state adversaries.

> ***More adversaries have gained the ability to inflict harm on the homeland, and the US must contend with increases both in the number of potential targets it must defend and in the variety of methods it must defend against.***

Regional powers: Iran and North Korea

Iran's current nuclear capabilities remain unclear, but the country has conducted cyberattacks on US critical infrastructure and is a longtime state sponsor of terrorism. In late 2024, the US Department of Homeland Security reported that Iran "maintains its intent to kill US government officials it deems responsible for the 2020 death of its Islamic Revolutionary Guards Corps-Qods Force Commander and designated foreign terrorist Qassem Soleimani" and "will continue to

[1] In our descriptions of threat actors in this section, we focus on the actors' current capacity to target the US, omitting discussions of likely future developments or intentions.

target US critical infrastructure, among other targets."[2] In addition, Iran has a significant conventional military capability that it wields regionally, and it actively supports regional non-state actors such as Lebanese Hezbollah, the Houthis, and Shia militias in Iraq and Syria, all of whom who have called for violence against the US.

North Korea is developing and testing nuclear weapons and ballistic missiles that can reach the continental United States and has a proven cyber capability that can target the domestic assets and infrastructure of the US. Although North Korea cannot project conventional military forces to the United States, it is using its vast conventional military to threaten South Korea. North Korea's unpredictable leadership and aggressive rhetoric could lead to a regional war or an international conflict that involves and could ultimately threaten the United States.

Global powers: China and Russia

China's advanced cyber activities against and propaganda efforts in the US—including penetrating critical infrastructure, stealing intellectual property, and conducting influence operations—are jeopardizing US economic security and disaster response. Since the early 2000s, China has rapidly expanded its military, including its nuclear arsenal, and it has begun to string together a network of overseas bases and economic holdings (e.g., ports and key infrastructure) that enable it to threaten US security at a level on par with that of the former Soviet Union.

Russia's cyber capabilities and information operations allow it to target critical American infrastructure and social media. In addition, Russia has employed irregular means, such as assassinations, to target individuals in other countries around the world, including in the West. Finally, Russia can threaten the United States with its conventional military forces, such as its submarines and bombers, and it has the world's largest nuclear arsenal, which can hit the United States less than an hour from launch.

Likely targets

The United States has numerous targets, including transportation nodes, supply chains, military bases, lifeline services, and American unity.

Transportation nodes, including airports, seaports, rail terminals, and highway interchanges, facilitate efficient logistics and supply chain operations, support economic growth, and ensure the timely delivery of essential resources and people. In wartime, transportation nodes are critical to move the joint forces from the US to the battlefield and are high-priority targets for adversaries. Disruptions to these nodes could have far-reaching effects on everything from daily commutes to global trade, highlighting the importance of the nodes to national security and economic stability.

Supply chains—especially those that are part of the defense industrial base—are extremely important in any conventional conflict. Disruptions to the US supply chain could hinder military capabilities, compromise mission success, and reduce overall strategic advantage. In addition, the increased reliance of the US on global commerce and just-in-time supply chains to keep civilian food and pharmaceutical shelves full make the supply chains attractive targets.

Military bases are also prime targets. Striking these facilities could significantly weaken US military strength, disrupt operational planning, and reduce the ability of the US to respond effectively. In addition, targeting military facilities can affect military members psychologically, lowering morale and creating chaos within the ranks, thereby further diminishing combat effectiveness.

[2] *Homeland Threat Assessment*, Office of Intelligence and Analysis, Department of Homeland Security, Oct. 2, 2024, pp. 4, 22, https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf.

Lifeline services, which include power, water, communications, and financial operations, remain vulnerable on several fronts. The US relies on operational technology (OT) to operate the critical infrastructure that enables lifeline services, including systems and devices used to manage and control industrial processes. OT enables real-time monitoring and automation of complex operations, but these systems are vulnerable to cyberattacks. At the same time, critical US infrastructure is both physically aging and becoming obsolete, especially as more people concentrate into urban and suburban areas.

American unity in the face of conflict, even one that spills over into the US, cannot be taken for granted. Public support and political backing are essential to ensure the success of sustained military operations and resource allocation efforts, but attacks on the homeland that take American lives, destroy cultural symbols, and cause economic harm are not guaranteed to unite the American people. These disruptions, particularly when exploited by influence operations, can lead to discord, which could erode support for US military operations.

Possible vectors

Cyberattacks have become increasingly common since the turn of the century, and state adversaries have shown their ability—and, in times of conflict, their intent—to exploit increased US reliance on both OT and the internet of things to attack critical infrastructure, lifeline services, and information technology.

Information operations have taken on new significance since the rise of social media permanently altered the media landscape and increased US vulnerability to state adversary interference. Because state adversaries are now able to communicate directly with US citizens, they can attempt to influence the information Americans see and the interpretations that gain traction. Through such efforts, state adversaries can seek to interfere with disaster preparation and response, undermine confidence in government, or erode US cohesiveness and will to fight.

Sabotage can be an effective way to interfere with a nation's critical capabilities and may be used before or during a conventional conflict. State adversaries are likely to target US communications systems, especially satellites, undersea cables, transportation nodes, and military facilities.

Smaller scale kinetic attacks aim to cause panic, disrupt daily life, and undermine public confidence in security measures, and they can include the use of uncrewed systems (drones), improvised explosive devices, vehicle ramming attacks, active shooter incidents, and assassinations or kidnappings that target key individuals to instill fear and gain media attention.

Chemical, biological, and radiological attacks are similar to smaller scale kinetic attacks but include chemical (e.g., sarin, VX, mustard gas, phosgene), biological (e.g., anthrax, ricin), or radiological (e.g., dirty bombs) agents. These weapons require sophistication to employ, and the responses require specialized equipment and trained personnel, neither of which are readily available in all parts of the United States.

Conventional missile strikes pose a significant threat to the US because they can target and damage critical infrastructure, military installations, and civilian areas. Such attacks can cause substantial casualties, disrupt essential services, and create widespread panic, ultimately undermining national security and economic stability.

Nuclear weapons and dirty bombs can be used in regional conflicts, in limited strikes in the US, or en masse in a catastrophic nuclear exchange that results in massive destruction and loss of life. Adversaries may be tempted to use tactical nuclear weapons, which are smaller and more versatile and offer a lower yield than strategic nuclear weapons.

The trick is putting it together

By gaining familiarity with the three major elements of the threat picture—the actors, the targets, and the vectors—consequence managers can better anticipate which adversary activities are the most likely. These three components, however, must be examined within the context of the global threat environment; otherwise, consequence managers may struggle to understand when a given actor might use a given vector to attack a given target, as well as what types of response activities or protocols they might need to have in place.

The challenge lies in connecting what adversaries could do to how consequence managers should prepare, based on the prevailing global threat environment. To help address this challenge, CNA has loosely organized the global security environment into three phases: peacetime competition, crisis or escalation, and direct conflict.

Competition refers to regular, ongoing military and strategic activities that occur outside of major conflicts or crises. Competition activities may occur during "steady state," when US adversaries may engage in low-level activities to maintain political or economic influence, deter adversaries, test US resolve, and prepare for potential escalations.

Crisis or escalation refers to a situation in which adversaries engage in hostile activities against the US or its partners without direct, open warfare. Instead, these nations and groups use proxies, cyber operations, non-attributable kinetic operations, and other indirect means to achieve their strategic objectives and undermine their adversaries. This type of conflict allows nations to exert influence and pursue goals while limiting the risks and costs associated with direct military confrontation.

Direct conflict refers to a situation in which the US is engaged in open, direct military confrontation with one or more adversaries. This type of conflict involves the use of armed forces (e.g., ground troops, naval fleets, air power) to achieve strategic objectives and defeat the adversary. Direct conflict is characterized by major combat operations such as large-scale battles and direct attacks, and it often results in significant casualties and destruction.

The two tables that follow provide a framework for "putting it all together." Table 1 focuses exclusively on capabilities and captures threat actor capabilities with a range of outcomes (i.e., from causing a nuisance to having catastrophic consequences), organized by the type of vector that different threat actors would use in an attack. Table 2 focuses on the likelihood of specific types of targets being attacked and the level of attack that should be anticipated during three different threat environments (competition, crisis, and direct conflict). This second table is less concerned with which threat actor might attack than with the likelihood that an attack of that kind might occur at all.

Table 1. Threat actor capability

Vector	Disruption, minor *(Most likely)*	Disruption, major	Catastrophic *(Least likely)*
Nuclear weapons		🇨🇳 🇷🇺	🇨🇳 🇷🇺 🇰🇵
Conventional missile strikes		🇨🇳 🇷🇺 🇰🇵	🇨🇳 🇷🇺 🇰🇵
Chemical/biological/radiological		🇨🇳 🇷🇺 🇰🇵	🇨🇳 🇷🇺 🇰🇵
Smaller-scale kinetic attacks	🇨🇳 🇷🇺 🇰🇵 🇮🇷	🇨🇳 🇷🇺 🇰🇵 🇮🇷	🇨🇳 🇷🇺 🇰🇵 🇮🇷
Cyber-attacks	🇨🇳 🇷🇺 🇰🇵 🇮🇷	🇨🇳 🇷🇺 🇰🇵 🇮🇷	🇨🇳 🇷🇺 🇰🇵 🇮🇷
Sabotage	🇨🇳 🇷🇺 🇰🇵 🇮🇷	🇨🇳 🇷🇺 🇰🇵 🇮🇷	🇨🇳 🇷🇺 🇰🇵 🇮🇷
Information operations	🇨🇳 🇷🇺 🇮🇷	🇨🇳 🇷🇺	

LEGEND
🇨🇳 China 🇷🇺 Russia 🇰🇵 North Korea 🇮🇷 Iran

Source: CNA.

Table 2. Probable targets by global security environment

	Targets	Disruption, minor *(Most likely)*	Disruption, major	Catastrophic *(Least likely)*
Peacetime	Transportation nodes	●		
	Supply chains	●		
	Military bases			
	Lifeline services			
	American unity	●	●	
Crisis or escalation	Transportation nodes	●	●	
	Supply chains	●	●	
	Military bases	●		
	Lifeline services	●		
	American unity	●	●	
Direct conflict	Transportation nodes		●	●
	Supply chains		●	●
	Military bases		●	●
	Lifeline services		●	●
	American unity		●	

Source: CNA.

About CNA

CNA is a not-for-profit analytical organization dedicated to the safety and security of the nation. With nearly 700 scientists, analysts, and professional staff across the world, CNA's mission is to provide data-driven, innovative solutions to our nation's toughest problems. It operates the Center for Naval Analyses—the Department of the Navy's federally funded research and development center (FFRDC)—as well as the Institute for Public Research. The Center for Naval Analyses provides objective analytics to inform the decision-making by military leaders and ultimately improve the lethality and effectiveness of the joint force. The Institute for Public Research leverages data analytics and innovative methods to support federal, state, and local government officials as they work to advance national and homeland security.

To learn more about civil defense and the ways that emergency managers can tackle planning challenges, contact civildefense@cna.org.

CNA