World War III

Union of Saints

A Modern Definition

World War III may be defined as a continuing global conflict involving conventional war, proxy war, nuclear threats, cyberattacks, espionage, terrorism, economic pressure, information operations, psychological warfare, organized criminal activity, and attacks against critical infrastructure. Under this definition, war is no longer confined to uniformed armies fighting on declared battlefields. It reaches Americans through government systems, businesses, hospitals, utilities, financial institutions, communications networks, social media, transportation systems, borders, neighborhoods, and private homes.

While the United States has not formally declared “World War III,” it means that current hostilities can be examined as an interconnected form of global hybrid warfare, gray zone conflict, political warfare, criminal proxy warfare, and fourth generation warfare. The participants may include governments, military forces, intelligence services, terrorist organizations, cyber groups, criminal networks, political movements, corporations, propagandists, and individuals acting as proxies.

Russia

Russia is engaged in a major war against Ukraine while retaining nuclear weapons, advanced missiles, undersea systems, cyber capabilities, espionage operations, information operations, and weapons capable of threatening space systems. Russia also uses gray zone tactics intended to pressure adversaries while remaining below the traditional threshold of declared war. The most dangerous possibility is an escalating confrontation that produces direct hostilities between Russia and the United States or NATO, including potential nuclear escalation.

Russian hostile activity may include cyber intrusion, intelligence collection, disinformation, political influence, infrastructure reconnaissance, proxy activity, military intimidation, sabotage, and efforts to weaken public confidence. These operations can be directed against governments, military organizations, private companies, elections, communications systems, and the public. The 2026 United States intelligence assessment identifies Russia as one of the most persistent and active cyber threats facing the country. 2026 Annual Threat Assessment

Cyber Targeting From Asia

“Asian cyber targeting” is stated precisely as Asia contains many countries, including American allies. The principal state cyber threats identified by the United States government

include the People's Republic of China and North Korea. China conducts extensive cyber espionage and has reportedly placed hackers inside or near American communications, energy, transportation, and water infrastructure to create possible disruption options during a future conflict.

North Korea operates a sophisticated cyber program involving espionage, cryptocurrency theft, financial crime, intelligence collection, and attacks intended to fund the regime and its weapons programs. The United States intelligence community estimates that North Korean cryptocurrency theft reached approximately $2 billion during 2025. China and North Korea also possess military, missile, space, intelligence, and asymmetric capabilities affecting the United States and its allies in the Pacific.

Iran and Other Hostile Actors

Iranian cyber actors have targeted American government agencies, businesses, infrastructure, and individuals. Iran has also used regional partners and proxy organizations to attack American and allied interests. Terrorist organizations, ideologically motivated attackers, ransomware organizations, and transnational criminal networks add another layer to the conflict.

Russia, China, North Korea, and Iran selectively cooperate when their interests align, while maintaining separate national goals. Their combined actions can still create simultaneous military, cyber, economic, intelligence, and homeland security pressures against the United States.

Hostile Conditions Affecting Americans

The present conflict may include:

1. Conventional warfare and military escalation
2. Proxy wars and foreign sponsored armed groups
3. Nuclear threats and missile development
4. Cyberattacks against government and private networks
5. Targeting of electricity, water, transportation, communications, and health care
6. Espionage and theft of military, commercial, medical, and personal information
7. Artificial intelligence assisted cyber operations
8. Ransomware and financially motivated cybercrime
9. Information warfare, propaganda, and disinformation
10. Psychological and cognitive warfare
11. Election interference and covert foreign influence
12. Surveillance, digital stalking, doxxing, and harassment
13. Theft of intellectual property and industrial secrets
14. Counterspace weapons and targeting of satellites
15. Economic warfare, sanctions, trade pressure, and supply chain manipulation
16. Biological and chemical weapons threats

17. Terrorism and extremist recruitment
18. Human trafficking, drug trafficking, weapons trafficking, and organized crime
19. Criminal proxy warfare and the weaponization of criminal networks
20. Sabotage and prepositioning for future infrastructure disruption
21. Border exploitation by terrorists, smugglers, and transnational criminal organizations
22. Weaponized migration when population movement is deliberately manipulated for strategic purposes
23. Strategic corruption and institutional infiltration
24. Politically sponsored criminality and engineered insecurity
25. Urban destabilization, riots, arson, looting, and organized violence when directed, financed, or exploited for political objectives
26. Attacks against military personnel, veterans, police officers, border personnel, public officials, and civilians
27. Attacks on financial systems, cryptocurrency markets, banks, and personal accounts
28. Cultural and social division deliberately amplified by hostile influence operations
29. Foreign efforts to weaken trust in American institutions and communities
30. Convergence between physical attacks and cyber operations

Important Evidentiary Standard

Crime, protest, migration, political disagreement, demographic change, and social disorder may constitute Fourth Generational Warfare. To classify an event as foreign or domestic directed warfare, criminal proxy warfare, or fifth column activity, evidence should establish coordination, financing, direction, material support, strategic exploitation, or another meaningful connection to a hostile government or organization.

Working Definition

World War III is a multidimensional global conflict conducted through conventional forces, proxy organizations, nuclear pressure, cyber operations, espionage, terrorism, economic coercion, information warfare, psychological operations, criminal networks, attacks on infrastructure, and other military and nonmilitary means. It is a world without pause in which the boundaries between foreign and domestic, military and civilian, physical and digital, and peace and war have become increasingly difficult to identify. Americans may experience this conflict through cyber intrusion, foreign influence, economic disruption, organized exploitation, terrorism, infrastructure threats, propaganda, foreign and domestic racial hostilities and the persistent targeting of national security, public safety, and social stability.