



CIVIL DEFENSE: FROM THE COLD WAR TO CONTEMPORARY THREATS

INTRODUCTION

Civil defense has played a critical role in national security for much of American history. From its origins in World War I Europe, through its establishment in the United States during World War II, and the heightened tensions of the Cold War, civil defense principles have been used to meet the threats faced by the United States. In the post-Cold War era, the emphasis on large-scale military threats diminished, and civil defense agencies evolved into today's emergency management organizations. In subsequent years, the term *civil defense* fell out of use by federal agencies, states, and local governments. However, the nation is facing renewed risk of foreign intervention on the homeland primarily from cyberattacks from foreign actors on our nation's critical infrastructure. Despite the obvious and immediate differences between a cyberattack and a traditional military attack, cyberattacks on critical infrastructure similarly might cause widespread effects resulting in loss of life and severely degrading or destroying societal functions. Given this pressing threat, the time is right for a renewed interest in civil defense from government agencies at all levels. This white paper explores the historical role of civil defense, its evolution over time, and the relevance of past strategies in addressing today's emerging threats and challenges.

DEFINING CIVIL DEFENSE

At the time of its inception, *civil defense* referred to activities designed to minimize the effects of war on the civilian population and deal with immediate emergency conditions caused by attack. Civil defense spans all phases of emergency response, including preparedness, immediate response, and longer-term response to and recovery from an attack on the homeland.

- **Preparation** of operational plans and supporting agreements, the recruitment and training of personnel, the conduct of research, the procurement and stockpiling of necessary materials and supplies, the provision of suitable warning systems, the construction or preparation of shelter, and evacuation plans for the civil population.
 1. **Immediate response** measures, such as regulatory enforcement; the evacuation of personnel to shelter areas; traffic and panic control; provision of emergency lighting during wide-spread power outages; and secondary and tertiary options for civil communications.
- **Ongoing response and recovery** activities, such as firefighting, rescue, emergency medical services, health and sanitation services, monitoring for specific hazards of special weapons, unexploded bomb reconnaissance, essential debris clearance, emergency welfare measures, and immediately essential emergency repair or restoration of damaged critical infrastructure.¹

¹ United States, *Federal Civil Defense Act of 1950*, 1951, <https://maint.loc.gov/law/help/statutes-at-large/81st-congress/session-2/c81s2ch1228.pdf>.



CIVIL DEFENSE DURING THE WORLD WARS

WORLD WAR I (1914–1918)

During World War I, Germany's air strikes targeting civilian populations were designed to deteriorate the British military power and the nation's will to wage war. The heightened fears of an attack on American soil laid the foundations for what would become civil defense.² As England was targeted by German air strikes, the lack of organized civil defense strategies increased the deadly effect of the bombing, as citizens were left to find shelter and safety on their own. It became clear to the world that civil defense, largely undeveloped at the time, would become a necessity during future wartimes.³

WORLD WAR II (1939–1945)

Although it has its roots in World War I Europe, civil defense formally emerged as a federal strategy in the United States in 1941, when President Franklin D. Roosevelt created the Office of Civilian Defense (OCD) to help defend and protect the United States from attacks on American soil.⁴ From the beginning of World War II, militaries on both sides targeted civilian populations and industries that supported the war effort. These civilian attacks and bombings in Europe led to concerns over the possibility of similar attacks on American soil. Both the public and local officials demanded civilian defense strategies. Civil defense efforts were established, including training volunteers, engaging the public in various safety drills and techniques, and focusing on natural disaster preparedness on top of wartime safety.⁵ Despite these successful preparedness efforts, by the end of war, many believed civil defense was no longer necessary. When President Harry Truman took office in 1945, his administration abolished the OCD, and civil defense was no longer considered a top priority.⁶

² Homeland Security National Preparedness Task Force, *Civil Defense and Homeland Security: A Short History of National Preparedness Efforts*, 2006, <https://www.govinfo.gov/content/pkg/GOVPUB-HS-PURL-gpo90314/pdf/GOVPUB-HS-PURL-gpo90314.pdf>.

³ Homeland Security National Preparedness Task Force, *Civil Defense and Homeland Security*.

⁴ "Federal Civil Defense Act of 1950, Encyclopedia.com," <https://www.encyclopedia.com/history/encyclopedias-almanacs-transcripts-and-maps/federal-civil-defense-act-1950>.

⁵ Patrick S. Roberts, "The Lessons of Civil Defense Federalism for the Homeland Security Era," *Journal of Policy History* 26, no. 3 (2014), pp. 354–83, <https://doi.org/10.1017/s0898030614000165>.

⁶ Homeland Security National Preparedness Task Force, *Civil Defense and Homeland Security*.



COLD WAR (1945–1991)

The Cold War and the concurrent development of the atomic bomb reignited fears about an attack on the American public on US soil and the possibility of mass population loss in the event of nuclear warfare.⁷ After a successful nuclear weapons test by the Soviets in 1949 and the public's and government officials' demands that the Truman Administration take action, a defense proposal called "The Blue Book" was created, which outlined civil defense activities to be implemented at every level of government and firmly recommended the creation of a permanent federal civil defense agency.⁸ This proposal paved the way for the establishment of the Federal Civil Defense Administration, which went on to perform many civil defense activities throughout the 1950s, such as leading shelter building programs, improving federal and state civil defense coordination, establishing early warning systems and civil defense drills for attacks, providing guidance for the construction of fallout shelters, producing civil defense movies for children, and creating a national civic education program.⁹

With the backdrop of a continued nuclear threat, coupled with a series of significant natural disasters threatening the safety, security, and economy of the nation, federal and state governments struggled to rapidly respond to and recovery from natural disasters, much less than manage the impacts of a ballistic nuclear missile attack. The federal government required a new framework and organization to manage both threats. The Federal Emergency Management Agency (FEMA) was established in 1979 under President Jimmy Carter with the goal of coordinating the federal government's response to natural disasters and man-made disasters, such as nuclear warfare.¹⁰ Initially, FEMA focused on preparing for nuclear attacks, managing fallout shelters and evacuation routes, and coordinating civil defense efforts between state and federal agencies.¹¹ After the end of the Cold War, as the need for comprehensive disaster response was necessary beyond typical civil defense at the time, the agency's priorities shifted toward natural disasters and related emergency management in disaster recovery and response. This shift marked a significant change in both FEMA's mission and in civil defense strategies as a whole.

POST-COLD WAR (1991–Present)

With the end of the Cold War and the reduction of nuclear threats, the focus of civil defense shifted to non-attack priorities, namely natural disaster response and recovery, especially following significant events such as Hurricane Andrew in 1992. The emphasis on large-scale military threats diminished, and civil defense agencies were restructured or absorbed into broader emergency management organizations. In the early 2000s and following the September 11 attacks in 2001, DOD and other federal agencies initiated a global war on terrorism to keep the threat overseas. Domestic priorities evolved to eliminate silos and increase

⁷ "Civil Defense Through Eisenhower," US National Park Service, https://www.nps.gov/articles/coldwar_civildefense_thru-ike.htm.

⁸ "Civil Defense Through Eisenhower."

⁹ "Civil Defense Through Eisenhower."

¹⁰ "History of FEMA," FEMA, Jan. 4, 2021, <https://www.fema.gov/about/history#>.

¹¹ Katherine Malus, "Nuclear Disaster: How Prepared Are We?" Columbia K=1 Project, Center for Nuclear Studies, Nov. 2, 2018, <https://k1project.columbia.edu/content/nuclear-disaster-how-prepared-are-we>.



coordination through the consolidation of intelligence agencies into fusion centers at the State level; homeland security and emergency management agencies under the Department of Homeland Security at the federal level; and homeland defense organizations under NORAD and the US Northern Command in North America. However, since the 1990s, the role of civil defense in national security again became less pronounced, and resources were often redirected toward other areas of emergency management.¹² For example, Hurricane Katrina in 2005 highlighted the pressing need for regional catastrophic preparedness against a backdrop of increasing frequency and impact of natural disasters.

CIVIL DEFENSE AND EMERGING THREATS

*Please bear in mind that up to this war and never in our history, has the civilian population been exposed to an attack. The new technique of war has created the necessity for developing new techniques of civilian defense.*¹³

—Fiorello LaGuardia to President Roosevelt (WWII)

In the modern landscape, new threats have emerged, presenting new challenges that traditional civil defense strategies were not originally designed to address. These emerging threats require an approach that integrates past civil defense principles with modern emergency management knowledge, frameworks, and innovation. In particular, the growing threat of cyberattacks on critical infrastructure from foreign actors provides an urgent example of the need for renewed interest in civil defense. Essentially, the homeland is no longer a sanctuary where nation-state threats maintain the capability today to influence the nation's environment including its critical infrastructure.

Critical infrastructure is vulnerable to attacks that can disrupt essential services, compromise sensitive data, and incite widespread panic among the population. In addition, the interconnected nature of technology means that a single incident or vulnerability can have far-reaching consequences, making preparedness and resilience more complex than ever. Meanwhile, the information environment has transformed dramatically, with social media, digital communication, and technology-based tools reshaping how information is disseminated and how response is conducted. This shift presents additional challenges, namely the rapid spread of mis-/dis-/mal-information (MDM). MDM can exacerbate public fear and panic and can complicate emergency management and public health response efforts.

¹² Homeland Security National Preparedness Task Force, *Civil Defense and Homeland Security*.

¹³ Homeland Security National Preparedness Task Force, *Civil Defense and Homeland Security*.



INTEGRATING PAST STRATEGIES INTO MODERN PLANNING

Emergency managers around the country must adapt to these multifaceted and interconnected threats, with an emphasis on collaboration across sectors and levels of government. Despite the ever-evolving threat landscape, many principles from past civil defense strategies remain relevant, including the following:

- **Public communications mechanisms and messaging:** Effective public communication mechanisms are essential in increasing awareness of and preparing for cyber threats and infrastructure vulnerabilities. While civil defense in the Cold War relied heavily on centralized messaging and educational campaigns such as community drills to prepare for nuclear threats, today's strategies should adapt to modern threats by implementing public educational campaigns about cybersecurity and MDM, engaging local communities and private sector in planning efforts, and fostering public trust in federal activities and defense measures.
- **Operational plans:** In the Cold War era, operational plans were crucial to civil defense and encompassed air raid responses and evacuation measures to ensure coordinated responses to attacks. Today, effective operational plans remain a necessity but should evolve to include responses to a broader range of threats, particularly *sustained* cyberattacks. In an age of information acceleration, modern intelligence organizations must be able to quickly assess the complexity of a cyberattack and plans must be flexible and able to adapt to our rapidly changing technological environment, such as one in which communications, transportation, or critical lifeline services (e.g., water, electricity) are not available. As our government has grown to face new threats, defining roles for all stakeholders in a crisis and coordinating robust collaboration across sectors and public and private organizations will also be critical. To this end, the United States may require innovative approaches to supporting response operations through changes and/or exceptions to some regulations, laws, policies, and funding mechanisms. In addition, instead of stockpiling physical supplies like in past civil defense planning, current planning must prioritize the just-in-time procurement of both physical supplies and essential security and cybersecurity tools to ensure that the population can adapt and recover quickly from attacks. Finally, operational planning should include mechanisms for diversifying regular supply chains and supporting continuity of services, which will necessarily include more meaningful and proactive engagement of private sector partners before and during incidents with widespread impacts.
- **Recruitment and training of personnel:** During the Cold War, both recruitment and training of personnel were central to civil defense efforts, including extensive training programs to equip individuals with the knowledge needed in the case of a nuclear attack. Today, this focus on recruitment and training is even more important as threats have become especially diversified and specialized, as in the case of coordinated cyberattacks. Continuous recruitment and training of cybersecurity personnel will ensure that technical and physical consequences of an attack are addressed efficiently. A well-trained workforce can identify vulnerabilities and respond to incidents quickly. Training programs must evolve to incorporate new technologies and cybersecurity strategies, whereas physical security training must adapt to prepare citizens to take part in the physical security of buildings and directing traffic in the case of



widespread system outages. Effective volunteer management will still be critical and must include recruitment of qualified volunteers, effective trainings, and intentional integration of volunteers into response plans to support continuity efforts. Volunteers will be essential in enhancing response capabilities through providing additional manpower, security, and delivery of supplies, helping to supplement services that are normally managed using technology and fewer staffing requirements.

- **Essential emergency repair and restoration of damaged critical infrastructure:** Developing protocols for emergency repairs will ensure that essential services can continue during crises and that disruption to the community is minimized. Historically, effective civil defense responses have prioritized restoring services like electricity, water, and transportation to simultaneously facilitate recovery and ensure public safety. Today, the need for efficient repair and restoration processes is just as pressing. Modern threats require not only swift physical repairs but also the integration of technology to enhance infrastructure resilience and identify cyber vulnerabilities quickly. The private sector will need to play a role in this process because many private organizations have the expertise, resources, and equipment necessary for effective restoration, and strong and well-defined partnerships with these private entities ensure that critical resources and services are mobilized efficiently in an emergency. The Defense Production Act of 1950 can be leveraged to prioritize the production and allocation of resources and services, which can allow the government to compel private organizations to support urgent repair efforts.¹⁴

THE BLUE BOOK PROJECT: SUPPORTING MODERN PLANNING

The pressing threat from adversaries exploiting vulnerabilities in our nation’s critical infrastructure calls for a renewed focus on civil defense. The Virginia Department of Emergency Management’s Blue Book Project has undertaken a major effort to develop a coordinated operational process to secure critical infrastructure, support state and federal operational priorities, support our residents, and ensure continuity of government while under a coordinated cyberattack resulting in a national emergency. The threats addressed by the Blue Book Project highlight the need for a renewed focus on civil defense from federal, state, and local agencies.

The Blue Book Project closely resembles the nuclear-minded civil defense planning of the past. Like the unprecedented nuclear threats during the Cold War, a major cyberattack on critical infrastructure will be unprecedented in scale, will affect entire communities in ways that typical all-hazards planning does not account for, and will result in a severely degraded environment and widespread effects on day-to-day lives. In planning the response to and mitigation of a similar attack, plans will need to incorporate civil response strategies of the past as well. Response will require the full mobilization of US resources, major coordination between public and private entities, and a concerted public affairs and communications effort.

¹⁴ The Blue Book Project has a white paper specifically discussing the Defense Production Action. Please ask the contact listed at the end of this document to obtain a copy.



CONCLUSION

Threats change over the years, but many of the principles of civil defense, rooted in historical strategies from its inception, remain relevant for the modern risk landscape and emerging threats. By revisiting, leveraging, and modernizing these practices, emergency managements can gain advantage in planning, preparing, and safeguarding their communities from today's threats, including cyber threats to critical infrastructure.