21st Century Homeland Defense & Civil Defense

An Analytical Study

May 2nd, 2023

Rick White, Ph.D.
Arthur J. Simental, M.S.
John Holst, M.S.

Homeland Defense Institute

"Whether you like it or not, history is on our side. We will bury you."
- Nikita Khrushchev, November 1956

This publication was sponsored by the Homeland Defense Institute. The views expressed in this publication do not necessarily represent the views of the United States Air Force Academy, North American Aerospace Defense Command and United States Norther Command, the Department of Defense, or the United States Government.

"Here's my strategy on the Cold War: we win, they lose."
- Ronald Reagan

Abstract

War in the Ukraine has raised the prospects of a nuclear exchange between Russia and the US to a height not seen since the Cold War. In pursuing their own national interests, China and North Korea have also raised the nuclear stakes. Homeland Defense and Civil Defense both have the avowed mission of protecting the domestic US population from deliberate attack. Homeland Defense for the continental US is a shared responsibility between United States Northern Command and United States Strategic Command under the Department of Defense. Civil Defense is the responsibility of the Federal Emergency Management Agency under the Department of Homeland Security. The current Homeland Defense Strategy is resilience. The current Civil Defense strategy is resilience. Homeland Defense and Civil Defense also share a causal relationship: Civil Defense is what happens when Homeland Defense fails. This does not mean they can't be mutually supporting. This study takes a look at both Homeland Defense and Civil Defense to see how and why they have evolved to their present state. It then answers the question asked of this study, "How can USNORTHCOM support Civil Defense?"

“In war, prepare for peace, in peace, prepare for war.”
- Sun Tzu, The Art of War

Table of Contents

Executive Summary

War in the Ukraine has raised the prospects of a nuclear exchange between Russia and the US to a height not seen since the Cold War. In pursuing their own national interests, China and North Korea have also raised the nuclear stakes. Even if these countries choose not to risk a nuclear war with the US, they might still venture other forms of strategic attack to achieve their national objectives. Although a nationwide EMP or cyber attack against the US might not inflict the destruction of a nuclear attack, the consequences would still be catastrophic. How can US citizens be protected from any such attack?

Protecting the US population from attack is a primary responsibility of Homeland Defense. Homeland Defense has been a concern since the founding of Jamestown in 1607. The US Army and US Navy have fought to protect American interests and territory since 1775. The threat of direct attack on the US by conventional military forces diminished significantly after World War II in 1945. However, the threat of direct attack on the US with long-range nuclear weapons became an increasing reality after the Cold War with the Soviet Union began in 1947. Technical challenges made early anti-ballistic missile systems impractical, so the US relied on a strategy of retaliation to deter nuclear attack until the end of the Cold War in 1991. Confronted with the challenge of coordinating US defenses across four different commands, President Bush revised the Unified Command Plan after 9/11. USNORTHCOM was created and charged with the conventional defense of the continental US. USSTRATCOM retained control over the US nuclear triad. USCYBERCOM was later created to conduct offensive and defensive cyber operations. Even after 9/11, US defense strategy remains predicated on deterrence and the threat of direct conventional attack by a foreign power is still unlikely, which is why, in part, USNORTHCOM has no permanent assigned forces. However, USNORTHCOM does have a role to play in US deterrence strategy. According to the 2022 National Defense Strategy, one of the key aspects to Homeland Defense Strategy is resilience.

Civil Defense is also responsible for protecting the US population from attack and has also undergone significant evolutionary change. The 1950 Civil Defense Act created an agency to coordinate Federal efforts and assist State and Local governments with protecting citizens from nuclear attack. Fallout shelters were deemed the best means for surviving nuclear attack, but they were also considered too expensive and never publicly funded. Urban evacuation was a cheaper alternative, but it was also less effective and never seriously exercised. As public support waned, the Nixon Administration introduced a “dual use” policy whereby Civil Defense funds could also be applied towards Emergency Preparedness projects. In 1979 President Carter issued Executive Order 12148 creating the Federal Emergency Management Agency to coordinate Federal efforts and assist State and Local governments with protecting citizens from natural disasters. In 1993 the Civil Defense Act was repealed after the end of the Cold War. Following 9/11, FEMA was made part of the new Department of Homeland Security. Absent the threat of nuclear war, the remaining Civil Defense authorities transferred to FEMA in 1988 were subordinated to Emergency Preparedness. They had to be. The frequency and severity of natural disasters have grown fourfold since the 1980s. Since 2003 FEMA has used Homeland Security Grant Program funding to better prepare State and Local governments for disaster. Since 2005 the basic strategy of the National Preparedness Goal has been resilience.

FEMA has gotten quite proficient at helping State and Local governments prepare and respond to natural disaster. The problem is even the largest natural disasters are only regional. Large parts of the nation remain unaffected and provide a safe haven from where disaster assistance can be deployed. This would not be the case following a nationwide nuclear, EMP, or even Cyber attack. There would be

no safe havens from where to mount assistance. FEMA would be overwhelmed. The National Response Framework would likely fail. States would be on their own. State Governors would need every resource at their disposal to restore basic services and deliver food, water, and medicine. They would likely hold on to their National Guard. They would likely ask for assistance from local military installations.

Military installations have manpower, supplies, and transportation that would prove most helpful to State Governors following a nationwide attack. DOD Directive 3025.18 gives local commanders immediate response authority to save lives and prevent suffering. However, in the wake of a nationwide attack, local commanders might be understandably reluctant to share their resources. In the wake of a nationwide attack, Defense Support of Civil Authorities might be the key to resilience that the 2022 National Defense Strategy says is essential to Homeland Defense. But how will USNORTHCOM perform DSCA when FEMA is overwhelmed and the nation is in shambles? Perhaps they can adapt and improvise as they did following Hurricane Maria in 2017. Or perhaps better, they can plan ahead and have authorities and procedures in-place so local installation commanders don't have to wait on orders when the State Governors come asking for assistance.

The absence of permanently assigned forces and Posse Comitatus present challenges to developing DSCA contingency plans, but nothing that can't be overcome. Or perhaps such plans already exist, but when was the last time they were updated? And equally important, when was the last time they were exercised with FEMA? Although FEMA created the National Disaster Recovery Framework, exercises still tend to focus on regional disasters, not ones that are nationwide. USNORTHCOM might want to broker discussions with FEMA promoting exercises that examine what happens when the National Response Framework fails. USNORTHCOM might also want to participate and use this opportunity to gain insight to State and Local requirements to help develop or update DSCA contingency plans.

What about fallout shelters? They were deemed the most effective means of protecting the domestic population from nuclear attack. It seems a national program to build fallout shelters would receive no more public support today than it did during the Cold War, perhaps even less. What about improved anti-ballistic missile defenses? USNORTHCOM already has operational control over 44 missiles deployed to Vandenberg Air Force Base and Fort Greeley. Unfortunately, they are insufficient to counter a mass strike by Russia or China, and perhaps even North Korea. For understandable cost reasons the current system is a shadow of the one envisioned by the Strategic Defense Initiative. Perhaps forty years of technological advances, particularly in reusable rockets could produce a more capable missile defense within an acceptable cost range that could eliminate or greatly reduce the need for fallout shelters. As part of its Homeland Defense responsibilities, USNORTHCOM could lend its voice to those already advocating for an upgraded and improved national missile defense capability.

Homeland Defense and Civil Defense share a similar strategy, resilience. Homeland Defense and Civil Defense also share a causal relationship: Civil Defense is what happens when Homeland Defense fails. This does not mean they can't be mutually supporting. USNORTHCOM can work with FEMA to enhance State and Local resilience following nationwide attack, and in return, improved resilience can raise a potential attacker's opportunity costs and reduce their expected benefits to help deter attack on the US homeland.

Introduction

When Russia invaded Ukraine on February 22, 2022, most observers thought Russian forces would overwhelm Ukraine defenses and take the country within a matter of weeks. Russia opened its offensive with overwhelming force using combined air, missile, ground, sea, and cyber attacks. Outnumbering the Ukrainian Armed Forces 2-to-1, Russian infantry and armor spearheads advanced on four fronts towards the heart of the country. Supplied with Western anti-tank Javelins and anti-aircraft Stingers, Ukraine forces mounted a fierce defense that against all expectations halted the Russians in their tracks. Ukraine surprised the world and not only held off the Russian onslaught, but also started pushing them back. What was supposed to be a quick victory turned into a long stalemate. Infuriated over the standoff, Russian President Vladimir Putin warned he would use "all available means to protect the Russian people" to include nuclear weapons against the US. President Putin's remarks raised the prospects of a nuclear exchange between Russia and the US to a height not seen since the end of the Cold War. It also raised questions about the current state of US Civil Defense, and of specific interest to our customer, how they might best support it from United States Northern Command.

Part 1: Threats to the Homeland

After the threat of World War III subsided with the end of the Cold War, it seemed the threat of nationwide devastation had also disappeared. Even considering the worst case scenario of terrorists acquiring nuclear weapons did not pose the threat of nationwide devastation. However, in 2010 DHS noted the emergence of a new threat that could potentially inflict nationwide devastation, and perhaps more troubling, did not require the resources of a nation-state to unleash. That threat was cyber-attack.

Cyber Threat

9/11 demonstrated the ability to create WMD effects without using WMD. It was done by subverting US critical infrastructure. All critical infrastructure, particularly water, energy, transportation, and communications, what are considered "lifeline infrastructure", are vulnerable to cyber-attack. Experts believe a coordinated cyber-attack on critical infrastructure could precipitate the worst disaster in US history. The top -three concerns are 1) shutting down the North American electric grid, 2) instigating two simultaneous nuclear meltdowns, and 3) undermining the Federal Reserve. Like homeland security, cybersecurity emerged as a concern after the 1995 Tokyo Subway Attacks. Because they struck at Japan's critical infrastructure, a Presidential Commission was chartered to look at the safety and security of US critical infrastructure. The 1997 report noted that US infrastructure was safe, for the moment, but that it was becoming increasingly reliant on computer controls that might one day make it vulnerable to cyber-attack. As a result, in May 1998 President Clinton issued Presidential Decision Directive #63 (PDD-63) establishing the foundation for critical infrastructure protection from all threats, including cyber-attack. Concern remained sufficiently strong following 9/11 that the 2002 Homeland Security Act made cybersecurity a core mission for DHS, and it remains so to this day. However, because DHS was focused on a repeat 9/11-type physical attack, cybersecurity did not receive equal attention. That changed in 2010 with release of the first Quadrennial Homeland Security Review (QHSR). The 2010 QHSR elevated cybersecurity to top priority. The elevated priority is believed to stem from the 2008 Russian invasion of Georgia which was preceded by a cyber-attack that succeeded in

degrading the county's command-and-control. 2010 also saw the Pentagon attacked by a virus that gained access from a memory stick into their classified networks, and news that STUXNET had set back the Iranian nuclear program by physically damaging equipment inside a secure processing facility. [1]

To be sure, the cyber threat grew as the Internet grew, starting about the Third Epoch in 1995 when the introduction of the worldwide web saw the Internet balloon from 16 million to 4 billion users. From the start we knew the Internet was imperfect, but we embraced it despite its flaws. Bill Gates famously commented "If General Motors had kept up with the technology like the computer industry has, we would be driving $25 cars that got 1,000 miles to the gallon." GM famously responded "Yes, but for no reason whatsoever, your car would crash twice a day. Every time they repainted the lines on the road, you'd have to buy a new car. And your air bags would ask 'Are you sure?' before deploying." Still, on the whole, we embraced the Internet because it made everything better, faster, cheaper. Now, so many necessities of urban life depend upon the Internet that there's no way of going back to without it. So why is it so vulnerable? Two reasons: 1) all software is flawed, and 2) all humans are fallible. As a result, hackers are constantly searching for software bugs they can exploit, or if that proves too difficult, trying to trick users into releasing their legitimate access codes through phishing attacks. Unfortunately, none of these problems is fixable with current technology, nor are there any solutions in the foreseeable future. In the absence of a cure for cyber-attack, the nation must maintain continual vigilance to protect against new exploits and incessant phishing attacks. Cybersecurity, though, is a chain that's only as strong as its weakest link. It takes a village to maintain cybersecurity, and only one village idiot to destroy it. [1]

Although the 2002 Homeland Security Act tasked DHS with providing cybersecurity to the nation, the Department is not matched to meet the escalating threat. First off, DHS has no authority to touch anybody's computer, and they don't control the Internet. They do, however, maintain 24-hour watch over the Internet from the National Cybersecurity and Communications Integration Center (NCCIC) in Washington DC. If the NCCIC detects a problem, it may dispatch teams from either the US-CERT or ICS-CERT. The US Computer Emergency Readiness Team (CERT) at Carnegie Melon University has few deployable assets and is mainly positioned to collect and distribute malware reports. The Industrial Control Systems CERT (ICS-CERT) at Idaho National Laboratories does have deployable assets but can only respond with permission from system owners and operators. Likewise, the 13 DOD Cyber Mission Force teams dedicated to protecting the nation's infrastructure are similarly impeded. In short, there's no cavalry waiting over the hill to swoop down and rescue us from cyber-attack. As it stands, system owners and operators are the first and last line of defense from cyber-attack. [1]

International Threats

Nine nations possess nuclear weapons: China, France, India, Israel, North Korea, Pakistan, Russia, United Kingdom (UK), and the United States. When Mr. Lucie wrote his inciteful analysis in 2017, only Russia had directly threatened nuclear attack against the US under control of the former Soviet Union. That threat ended with the Cold War. Despite some major differences, none of these nations had the means or motive to instigate nuclear attack upon the US in 2017. All that changed in 2022.

Russia

On February 24, 2022, Russia invaded Ukraine. Tensions between the two countries had been building since February 2014 when protestors in favor of joining the European Union (EU) ousted President Viktor Yanukovych for seeking closer ties with Russia. Claiming to protect the rights of Russian

citizens, in March 2014 President Vladimir Putin deployed Russian forces to Crimea and took it away from Ukraine. Two months later, pro-Russian separatists in the eastern Ukraine regions of Donetsk and Luhansk declared their own independence. Armed conflict broke out between Ukraine and Russian-backed rebels in the region. Attempts to negotiate a peaceful settlement resulted in intermittent cease fires but no permanent resolution. In October 2021, US Intelligence reported more than 100,000 Russian forces massing along the Ukraine border. At 5:00 am on February 24, 2022, President Putin announced the start of a "special military operation" in Ukraine. [2]

Russia opened its offensive using combined air, missile, ground, sea, and cyber attacks. Infantry and armor spearheads advanced on four fronts, from the north towards Kiev, from the south towards Mariupol, and from the east and southeast towards Luhansk and Donbas. They were met by Ukrainian Armed Forces (UAF) supported by volunteers from the Territorial Defense Forces (TDF). By the numbers, Russia outmatched Ukraine in every way: Russia could draw on 900,000 active troops, four times more than the 196,000 in Ukraine; Russia had 15,857 armored fighting vehicles compared to 3,309 in Ukraine; and Russia had 1,391 combat aircraft compared to the 132 in Ukraine. [3] It was expected to be a very short war and the outcome inevitably in favor of Russia. But the numbers didn't capture Ukraine's advantages in morale, experience, and leadership. Both the ranks of the UAF and TDF were filled with combat veterans with years of experience fighting Russian-led rebels in the eastern provinces. At the head of Ukraine's military was President Volodymyr Zelensky, a young and vibrant leader who's defiance of Vladimir Putin garnered worldwide admiration and support. Supplied with Western anti-tank Javelins and anti-aircraft Stingers, Ukraine forces mounted a fierce defense against the Russian invasion. The combination proved effective in halting the Russian advance from the north, slowing its advance from the south, and eventually pushing back the advances from the east and southeast. [2]

The United States, member states of the North Atlantic Treaty Organization (NATO) and the European Union, and other partners regard Russia's war against Ukraine as "unprovoked and unjustified." The United States, the EU, and the United Kingdom, among others, have coordinated efforts to impose a series of increasingly more severe sanctions on Russia. They also have provided substantial military and economic aid to Ukraine. To deter further Russian aggression, the United States and NATO also have increased their military presence in Central and Eastern Europe. [4]

As Russia's invasion stalled, President Putin turned his anger towards the West. In a speech on September 21, 2022, Putin accused the West of plotting to destroy Russia and allegedly discussing the potential use of nuclear weapons against Moscow. He warned that he would use "all available means to protect Russia and our people". Putin further iterated that "This is not a bluff. And those who try to blackmail us with nuclear weapons should know that the weathervane can turn and point towards them." On September 30, 2022, President Putin justified his threats by saying the United States had created a "precedent" by dropping atomic bombs during World War II. [5]

President Putin's threats resurrected the prospect of nuclear war not experienced since the end of the Cold War. Is he serious? Since the Soviet Union detonated its first nuclear bomb in 1949, Moscow has promised to use nuclear weapons to defend its territory. Russia's nuclear doctrine allows for a nuclear strike after "aggression against the Russian Federation with conventional weapons when the very existence of the state is threatened." On September 30, 2022, Russia formally annexed about 18% of Ukrainian territory. Would Putin consider the continued export of US weapons to Ukraine an attack on Russia? Ramzan Kadyrov, head of Russia's republic of Chechnya, said on October 1, 2022 that Moscow should consider using a low-yield nuclear weapon in Ukraine after a major new defeat on the battlefield. Russia's Foreign Minister, Sergei Lavrov said that the West is overreacting, that Putin has

been clear that Moscow's nuclear policy is defensive. That may be true, but President Putin conjured false defensive arguments for taking Crimea in 2014 and attacking Ukraine in 2022. Could he not conjure similar false defensive arguments to justify deploying nuclear weapons? The fact of the matter remains that Putin ordered Russia's nuclear forces onto high alter shortly after the invasion began. [5]

Unfortunately, Russia's invasion of Ukraine emboldened both China and North Korea to take actions that also raised the prospects of nuclear war.

China

The People's Republic of China (PRC) was founded in 1949 after Mao Zedong's communist forces defeated the nationalists under Chiang Kai-shek who fled to Taiwan and formed the Republic of China (ROC). Although possessed of a great army that fought Western powers to a stalemate in Korea in 1953, China under Mao's rule was riven by internal struggle that prevented it from achieving equally great economic success. Still, China became a nuclear power when it detonated its first atomic bomb in October 1964. After Mao died in 1976, successive leaders of the Chinese Communist Party (CCP) starting with Deng Xiaoping focused on market-oriented economic development and opening the country to foreign trade. The changes made China one of the world's fastest growing economies with 9% annual growth. By 2011, the PRC's economy was the second largest in the world. By 2021, an estimated 800 million Chinese had been lifted out of poverty and their living standards dramatically improved. [6]

In 2012, Xi Jinping became Chairman of the CCP and was elected to his first 5-year term as the country's President in 2013. In 2018 Xi won his second term, and in March of that year the National People's Congress abolished term limits opening the way for him to remain in power indefinitely. Since becoming President, Xi has worked to make China a global economic and military superpower. The Belt and Road Initiative (BRI) begun in 2013 has invested billions across Asia and Africa to develop an interconnecting global trade infrastructure and extend China's diplomatic influence. In 2017 President Xi embarked on a military modernization program with the goal of developing the ability to project power beyond China's borders by 2020, field fully modernized forces by 2035, and possess a world-class military by 2035. Since taking office President Xi has used his country's growing power to press border issues with India, assert territorial claims in the South China Sea, and seek repatriation of Taiwan which it considers its 23rd province. [6]

With the communist victory in the Chinese civil war in 1949, the Nationalist-controlled Republic of China government and 2 million Nationalists fled to Taiwan and claimed to be the legitimate government for all China based on a constitution drawn up in 1947. The US never formally recognized the Republic of China nor established an embassy in Taiwan. However, when the Korean War broke out, President Truman began sending economic and military aid to Taiwan and sent the US Seventh Fleet into the Taiwan Strait to discourage any invasion from the PRC. The US maintained favored trade and military relations with Taiwan over the next thirty years. That changed in January 1979 when the US formally recognized the PRC as the legitimate government of China to help counter political influences and military threats from the Soviet Union. However, in April 1979 President Carter signed the Taiwan Relations Act (TRA) stating that the US would provide Taiwan with arms and maintain the capacity to resist any use of force or coercion that would jeopardize the security, or social or economic system, of the people of Taiwan. The TRA bound the US by law to protect Taiwan. [7]

In August 2022, House Speaker Nancy Pelosi paid a formal visit to Taiwan, stating "The visit should be seen as an unequivocal statement that America stands with Taiwan, our democratic partner, as it defends itself and its freedom." [8] China responded by staging large-scale military live-fire

exercises in the Taiwan Straits featuring several ominous "firsts": 1) Joint exercises were conducted in seven key areas surrounding Taiwan and inside its territorial seas; 2) There was an unprecedented overflight of Taiwan by several Chinese short-range ballistic missiles; 3) Thirty combat aircraft crossed the centerline of the strait before returning to their bases on the mainland; 4) Military drones flew over Taiwan-occupied Kinmen and Matsu islands off the Chinese coast; and 5) Disinformation including fake images of a Chinese warship near Taiwan were spread across social media. [9] At the conclusion of its exercises, China released the latest in a series of White Papers on Taiwan. The white paper sought to convey that China's overall policy toward Taiwan has not changed—that China remains committed to peaceful unification and "one country, two systems". However, the new white paper specifies "use of force would be the last resort taken under compelling circumstances." This sentence was an addition not included in the 2000 Taiwan white paper or the 2005 Anti-Secession Law. [10]

President Xi did not denounce Russia's invasion of Ukraine. It is thought that he is patiently watching and carefully considering what lessons might apply to Taiwan. If he sees advantage to China, the question arises would President Xi fabricate a "compelling circumstance" in Taiwan as President Putin did in Ukraine?

North Korea

Over the past six years, North Korea's advances in nuclear weapons and missile capabilities under its leader Kim Jong-un have catapulted Pyongyang from a threat to US interests in East Asia to a potential direct threat to the US homeland. [11]

North Korea has posed one of the most persistent US foreign policy challenges of the post-Cold War period. Having made advances in its nuclear and missile capabilities under its leader, Kim Jong-un, North Korea has evolved into a grave security threat to the United States. The United States and North Korea (officially known as the Democratic People's Republic of Korea, or DPRK) began denuclearization talks in 2018, but those negotiations essentially have been frozen since February 2019, with little apparent prospect for a breakthrough. Meanwhile, North Korea simultaneously has continued to develop its nuclear and missile capabilities. Other US concerns include North Korea's cyberspace activities, conventional military capabilities, egregious human rights violations, international terrorism, and illicit activities such as money laundering and smuggling. [12]

According to the US intelligence community's 2022 Annual Threat Assessment, Kim Jong-un views nuclear weapons and ICBMs as "the ultimate guarantor of his totalitarian and autocratic rule of North Korea and believes that over time he will gain international acceptance as a nuclear power." In a speech at an April 2022 military parade, Kim said the country "will continue to take measures for further developing the nuclear forces of our state at the fastest possible speed." As in past statements, he underscored the primary mission of its nuclear forces is to "deter a war" while also emphasizing the survivability of its nuclear deterrent force and readiness to apply "nuclear combat capabilities in any situations of warfare." In a September 9, 2022, speech to North Korea's Supreme People's Assembly, Kim Jong Un said, "there will never be any declaration of 'giving up our nukes' or 'denuclearization,' nor any kind of negotiations or bargaining to meet the other side's conditions." He vowed the country would continue developing its "nuclear power." The Assembly adopted a new law that reportedly expands the conditions under which North Korea would use nuclear weapons to include non-nuclear attacks and situations that threaten the regime's survival. [11]

Despite a long-standing United Nations ban on "all ballistic missile tests" by North Korea, the country continues to flight-test a variety of systems, advancing the reliability and precision of its missile

forces, and improving its ability to defeat regional missile defense systems. North Korea has publicly announced plans to develop and test new delivery vehicles. At the 8th North Korean Workers Party Congress in January 2021, Kim announced North Korea would field a new nuclear-capable submarine, develop its tactical nuclear weapons, deploy multiple warheads on a single missile, and improve its ICBMs' accuracy, among other goals. North Korea accelerated its testing in 2022, flight-testing 30 ballistic missiles. On March 24, 2022, North Korea tested an intercontinental ballistic missile, its first ICBM launch since November 2017. In mid-April 2022, North Korea flight-tested a short-range "tactical guided weapon" that is nuclear-capable. South Korean government sources, as well as analysts using publicly available satellite imagery, detected North Korean activities to restore the Punggye-ri nuclear test site, which the regime had closed in 2018. These observations prompted predictions that North Korea would carry out its seventh test of a nuclear weapon, and its first since 2017. [11]

In 2022, North Korea resumed efforts to improve its ability to strike the continental United States with an ICBM, ending a nearly five-year pause in long-range tests. On March 16, a failed ICBM flight test exploded over Pyongyang. North Korea followed up with a second ICBM test on March 24, which it claimed was a Hwasong-17, but South Korean intelligence reportedly assessed it as a Hwasong-15 test. The US Defense Intelligence Agency assesses that the Hwasong-17 ICBM, first displayed at an October 2020 military parade, is "probably designed to deliver multiple warheads." On May 25, North Korea again test launched an ICBM, on the heels of President Biden's visit to South Korea and Japan. In early June, North Korea test-launched eight short-range ballistic missiles following the conclusion of a joint US-South Korea naval exercise. US Forces Korea and the South Korean military responded to that test launch by jointly firing eight ballistic missiles, similar to their response to the May 25 test. A US Forces Korea statement said the response was to "demonstrate the ability of the combined ROK-US force to respond quickly to crisis events." A South Korean Joint Chiefs of Staff statement said, "Our military's show of force was intended to highlight our resolve to firmly respond to any North Korean provocations, including an ICBM launch, and our overwhelming capability and readiness to conduct a surgical strike on the origin of the provocation." [11]

The war in Ukraine may lead Kim Jong-un to conclude that he has greater freedom of action. In the 1990s, Ukraine relinquished Soviet-legacy nuclear weapons in return for economic support and security guarantees from the United States, the United Kingdom, and the Russian Federation. Russia's breach of this agreement by invading Ukraine may strengthen arguments inside North Korea that denuclearization would increase the country's vulnerability to larger foreign powers. Additionally, perceptions of a trend toward an international system of zero-sum competition between two blocs—the United States and its allies and partners on one side, and China and Russia on the other—could embolden North Korea. Kim may conclude that if he uses the country's nuclear weapons and missile programs to coerce concessions from Seoul, Washington, and/or Tokyo, China and Russia would not take punitive actions against North Korea and may even provide economic assistance to preserve the DPRK's regime stability, similar to how they supported North Korea during the Cold War. In May 2022, China and Russia vetoed a US-led United Nations Security Council (UNSC) resolution that would have imposed new sanctions on North Korea in response to its ICBM tests. In the past, both countries had supported new UNSC sanctions resolutions following a DPRK ICBM test. [11]

In July 2022, the Senate Armed Services Committee cited North Korea's expanded nuclear and missile capabilities as part of the committee's justification for including provisions in the FY2023 National Defense Authorization Act (NDAA) that address the modernization of US nuclear weapons programs. The House version of the FY2023 NDAA includes a requirement that the Department of

Defense produce an annual public report on North Korea's military capabilities, similar to past NDAAs. [11]

Ukraine Nuclear Scenarios

Russia's invasion of Ukraine has raised the prospect of nuclear war for the first time in thirty years since the end of the Cold War. US nuclear strategy is deterrence. There are two schools of thought on the best approach to nuclear deterrence. The first school of thought is known as Simple Nuclear Deterrence, sometimes referred to as Minimum Deterrence. The thought is that deterrence is best achieved with a limited number of nuclear weapons that, for example, could destroy a certain number of an adversary's cities. The viability of deterrence is created by an adversary's fear of uncontrolled nuclear escalation. The second school of thought is known as Complex Nuclear Deterrence. This recognizes that nuclear deterrence can be more complicated, requiring an understanding of the adversary and various scenarios that could play out. This strategy also pays close attention to the nuclear balance and places a premium on ensuring the survivability of nuclear forces that can threaten the adversary. The complex nuclear deterrence approach has been the basis of US nuclear policy since about the 1960s, and it rests on presenting the president with a number of options and capabilities — particularly in a regional conflict — that would deter Russia's nuclear use in any scenario. [13]

In October 2022, National Security Advisor Jake Sullivan warned of "catastrophic consequence" should Russia deploy nuclear weapons. "US policymakers are wisely and deliberately ambiguous on how they would respond," said Daryl Kimball, executive director of the Arms Control Association. "There are many different scenarios that could involve nuclear use in that war, each of which would create unique circumstances, for which there is no simple, standard response." [14]

A 2019 simulation from Princeton University's Program on Science and Global Security shows a plausible step-by-step escalation of nuclear war between the US and Russia that starts in Europe. Under the simulation, Russia launches a nuclear warning shot from the city of Kaliningrad to halt US-NATO advances. NATO retaliates with a single tactical nuclear air strike. As the nuclear threshold is crossed, fighting escalates to a tactical nuclear war in Europe, with Russia sending 300 nuclear warheads via aircraft and missile, and NATO responding with 180 nuclear warheads shot from aircraft. The immediate casualty list reaches 2.6 million in more than three hours. NATO then responds with 600 strategic nuclear warheads shot from the US land and submarine bases, and Russia launches missiles from silos, road vehicles, and submarines. The immediate casualty count is 3.4 million in about 45 minutes. With the aim of inhibiting the other side's recovery, Russia and NATO target each other's 30 most populated cities, using five to 10 warheads depending on population size. Casualties from this move would reach 85.3 million in about 45 minutes. The overall number of immediate dead from the nuclear exchanges would reach 91.5 million, with deaths from nuclear fallout and other long-term effects significantly increasing the casualty number. [14]

The 1964 National Plan for Emergency Preparedness summarized post-attack conditions as follows:

> *"A nuclear attack, even one only on military and command centers, would cause widespread death and destruction from blast and heat effects, with heavy fallout probable over much of the country. In a large-scale attack any point in the United States could be damaged or contaminated. Nevertheless, there would be great variations in the amount and degree of devastation, and many areas would he completely free from these effects. Accurate prediction of these effects is impossible.*

Casualties. Loss of life would be enormous, especially in an attack on population centers, although fallout shelter and other protective actions could save tens of millions of lives. whatever the kind and degree of attack, human hardships and suffering would constitute the most serious immediate problem.

Effects on Resources. The most immediate requirements for human survival in the postattack period would be food and water. But studies indicate that usable supplies would be adequate postattack for supporting life.

Health resources-manpower, materials, facilities-would be in very short. supply and so, therefore, would health and sanitation services. Self-sufficiency on the part of the population would be necessary in maintaining health and caring for the sick and injured, perhaps for lengthy periods of time.

The most immediate economic results of nuclear attack, aside from direct loss and displacement of people and private property, would be the substantial loss of capital assets, disruption of the financial and credit structure, and shortages and maldistribution of manpower and materials.

Agricultural and industrial productive capabilities would be lost or denied and transportation and communication impaired, particularly as a result of the fire and fallout hazards in the early postattack period.

Losses of resources and productive capacity might, in some areas, be balanced by the number of deaths. Thus, under same attack patterns, the national supply of particular resources might be great enough to cope with, the overall demand. Rarely, however, would the surviving resources be where most needed.

Because of the interdependent nature of the Nation's economy, losses in damaged areas would soon be felt in undamaged ones. The total supply-requirements situation could be realistically assessed only by keeping in mind this interwoven economic and geographic relationship.

Effects on Systems. Normal systems of distribution, communication, transportation, production, power supply, finance, welfare, public services, law enforcement, and government aid could be disrupted in many areas for periods ranging from days to months. Hence survival and subsistence in such affected areas would depend for varying periods on local self-sufficiency.

Disruption of communications might. delay for several days even a gross assessment of the postattack situation for the entire country. More detailed surveys and assessments of population and resource status might not be feasible for some time. This would not, of course, prevent local damage assessment by direct observation and on-the-spot analysis. Radiation hazard would probably cause long-term denial of use and occupancy of some areas. This and other damage would restrict mobility between and within some localities and even regions. Most areas affected by fallout would, however, be accessible within 2 weeks.

In some areas the damage might be so severe and the radioactivity so persistent and intense as to require decisions whether to rebuild damaged cities or relocate them." [15]

"From the past games, we learned that it was difficult to de-escalate the situation and achieve the US's objectives," said Stacie Pettyjohn, senior fellow and director of the defense program at the Center for a New American Security. "One can always deescalate by capitulating but that is not what the

US is searching for." "Once nuclear weapons are used—even in a very limited fashion—escalation dynamics are dangerous and hard to predict," Pettyjohn added. [14]

Putin's use of even tactical nuclear weapons would lead to the opening "of the last destructive direction in relation to Russia, and there would be no chance for Russia to return to the club of countries, with which at least someone shakes hands," Ukraine's Minister of Defense Oleksii Reznikov said, according to Interfax Ukraine. [14]

Black Sky Event

A nuclear exchange with Russia, China, or Korea would have catastrophic consequences for the US. As described in the 1964 National Plan for Emergency Preparedness, the death and destruction caused by blast damage and radiation fallout would be compounded by the loss of critical infrastructure. Critical infrastructure are basic services needed to sustain society. Contemporary urban society that comprises 83% of the US depends on many interdependent infrastructures identified by Presidential Policy Directive #21 as follows:

1. Chemical	7. Emergency Services	13. Information Technology
2. Commercial Facilities	8. Energy	14. Nuke Reactors, Materials, & Waste
3. Communications	9. Financial Services	15. Transportation Systems
4. Critical Manufacturing	10. Food & Agriculture	16. Water & Wastewater
5. Dams	11. Government Facilities	
6. Defense Industrial Base	12. Healthcare & Public Health	

Table 1: Critical Infrastructure Sectors, 2013 PDD-21

Among the sixteen critical infrastructure sectors identified by PDD-21, four in particular are called "lifeline" infrastructure because they form the basis on which all others depend. The four lifeline sectors are communications, energy, transportation, and water. The four lifeline infrastructure sectors are mutually dependent; take away one and the others cannot function. Among these four, perhaps the most vulnerable and easiest to take away is the electricity subsector in the form of the North American Electric Grid. [1]

The loss of electricity over a wide region for a long duration is called a "Black Sky Event". The loss of the North American Electric Grid would be an extreme "Black Sky Event". A nuclear strike on the US would likely cause a Black Sky Event, but it is not the only means of shutting down the North American Electric Grid. Russia, China, and Korea have the ability to create a "Black Sky Event" using Electromagnetic Pulse (EMP) and Cyber-Attack. [16]

EMP is incidental to an atmospheric nuclear blast. EMP induces current within an electric circuit possibly causing it to fail from overload. EMP can disable a country's grid and also render many electrical items useless. The extent of EMP damage depends on the height of a nuclear detonation. A nuclear warhead detonated at an altitude of 18 miles would generate an EMP field on the ground with a radius of 372 miles. If an EMP attack was to be triggered at an altitude of 294 miles it would cover most of the US. A 2004 report by the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack determined "A single EMP attack may seriously degrade or shut down a large part of the electric power grid in the geographic area of EMP exposure effectively instantaneously. There is also a possibility of functional collapse of grids beyond the exposed area, as electrical effects propagate from one region to another… Should significant parts of the electrical power infrastructure be lost for any substantial period of time, the Commission believes that the consequences are likely to be catastrophic,

and many people may ultimately die for lack of the basic elements necessary to sustain life in dense urban and suburban communities." [17]

The North American Electric Grid is also vulnerable to cyber-attack. Like many other networks, the electric grid is managed using Supervisory Control and Data Acquisition (SCADA) systems. These may be attacked directly or indirectly using exploits or phishing schemes. In 2007, DHS conducted a joint experiment called Project Aurora demonstrating the ability to destroy an electrical generator from the Internet. In December 2016, cyber-attack succeeded in knocking out the power to the city of Kiev in Ukraine. [1] In April 2022, Russian cyber forces again attacked the electrical grid as part of their invasion of Ukraine. Russia's onslaught has been characterized as the "most sustained and intensive cyber-campaign on record." [18] US infrastructure has not been immune to cyber-attack. In March 2018, DHS issued an alert warning of Russian infiltration into the US Electric Grid. [1] In May 2021, hackers breached Colonial Pipeline's billing system demanding $4.4 million in ransom. To contain the virus the company shutdown its network supplying 45% of all fuel consumed on the US East Coast. Shortages affected fuel prices and availability across 17 States over the next week. [19]

Hurricane Maria

In September 2017, the US experienced a Black Sky Event when the Commonwealth of Puerto Rico was hit by Hurricane Maria. María made landfall on the southeast coast of the island near Yabucoa with winds of a Category 4 storm, on September 20, 2017. The hurricane's center crossed Puerto Rico diagonally from southeast to northwest exposing the Island to the hurricane's highest winds. The storm surge and wave action from María extensively damaged marinas and harbors along the east and southeast coasts. Heavy rainfall in excess of 15 inches over the next 48 hours caused the La Plata River to flood, stranding hundreds of families on rooftops. María knocked down 80 percent of Puerto Rico's utility poles and all transmission lines, resulting in the loss of power to the Island's 3.4 million residents. In the immediate aftermath the storm rendered 100 percent of the power grid, 95 percent of cellular sites, and 43 percent of wastewater treatment plants inoperable, and left less than 50 percent of the island with clean drinking water. [20] More than two months after Hurricane Maria devastated Puerto Rico, electricity had still not been restored to large sections of the island. Here are but some of the ways people were impacted:

- No Stoplights. Driving around after the storm was chaotic. Every intersection became a test of wills—the bold and reckless forged ahead, heedless of cross traffic, the meek waited for a break in traffic to make their move. Although a few of the busier intersections had traffic cops, the vast majority didn't. And the cops who had to stand out in the sun and the heat all day had a rough time in the heat wave that followed the storm.
- No Electronic Finances. After the storm hit, many ATMs didn't work at all for lack of power. Those that were still operating quickly ran out of money. Without money, consumers couldn't buy anything, and businesses couldn't sell anything. And of course, credit cards didn't work because there was no way to process transactions. The economy basically ground to a halt.
- No Cell Phones. The loss of cell towers and electricity disrupted cell service across the island. Going days without knowing the status of family members was a major source of stress.
- No Drinking Water. Electricity is essential for treating water to make it safe and running pumps to distribute it to homes. Contaminated drinking water resulted in widespread cases of vomiting, diarrhea, and pink eye. Clean bottled water became essential.

- No Refrigeration. Refrigeration is essential to preserving food and some medications. This is why ice became important. Without it, shopping became a daily necessity. Those shops that remained open were mobbed by long lines of people who waited for a very limited selection of goods.
- No Lights. No street lights or house lights or lights of any kind made it very difficult to move around at night because street signs were hard to read and buildings were indistinguishable from one another. [21]

The National Disaster Recovery Framework makes local governments primarily responsible for leading disaster recovery efforts. According to FEMA, however, the agency "essentially served as the first responder in the early response efforts in Puerto Rico," and provided many services "typically provided by territorial or local governments," including power restoration, debris removal, and commodity distribution. FEMA generally coordinates with state and local governments to manage commodity distribution, but Puerto Rico "did not have the same level of preparedness to manage a commodity distribution mission." As a result, FEMA took a more direct role than it usually does in commodity distribution. [20] The resulting response was the longest sustained air mission of food and water delivery in FEMA history. [22]

Hurricane Maria effectively shattered both the Puerto Rico Emergency Management Agency and the Puerto Rico National Guard (PRNG). The agency's staff members were unavailable and members of the PRNG and Puerto Rican Army Reserve (USAR)— many of whose homes had been damaged or destroyed—were initially preoccupied meeting the urgent needs of their immediate families and neighbors. In addition, the destruction of power and communications infrastructures and the limited mobility that the extensive debris left in the wake of the storm impeded the development of situational awareness and a common operational picture (COP). In effect, Hurricane Maria left the commonwealth unable to carry most of the burden of the needed response and recovery operations or to provide clear direction to Federal, DoD, and State response efforts. [23]

In late September, FEMA requested Defense Support of Civil Authorities (DSCA) from the Department of Defense. The Secretary of Defense (SecDef) gave the mission to United States Northern Command (USNORTHCOM) who has DSCA responsibility for US territory in North America and the Caribbean. USNORTHCOM designated US Army North (USARNORTH) the Joint Force Land Component Commander (JFLCC) and tasked them to conduct DSCA operations in Puerto Rico. They were immediately confronted by the challenge of operating in a decision-making vacuum at the local and commonwealth levels. DSCA operations are typically predicated on the assumption State and Local officials will make specific requests for assistance (RFAs) that, once authenticated, can then be translated into Mission Assignments (MAs) and MA task orders (MATOs) that address identified needs. The absence of a robust State and Local government required significant adaptation and improvisation on the part of USARNORTH, USNORTHCOM, and FEMA. USARNORTH conducted DSCA operations in Puerto Rico from September to November 2017. [23]

To help restore Puerto Rico's electric grid, on September 21, 2017 Puerto Rico's Governor Ricardo Roselló made an official request to New York's Governor Andrew Cuomo for emergency goods and services. The New York Power Authority (NYPA) quickly organized the New York State Contingent (NYSC) and deployed them the next day on September 22, 2017. Over the course of nearly eight months, the NYSC participated in five missions to the island during which numerous damage assessment and restoration efforts were conducted working closely with the Puerto Rico Electric Power Authority

(PREPA) and through the incident command structure that was established by the electric industry. The conditions on the ground in Puerto Rico would have tested even the most resilient and well-prepared utilities. Fundamental aspects of logistics, coordination, and communication were significantly undermined due to the extent of the destruction as well as on-island resource constraints, and the lack of an up-to-date local utility response plan and signed Mutual Assistance Agreements (MAAs). The extreme impact of the hurricane also illuminated the need for all stakeholders to focus greater attention on preparedness, training, and continuous improvement as fundamental aspects of emergency and mutual assistance planning. [24]

Puerto Rico had engaged in disaster preparedness exercises prior to Hurricane María; however, it had not recently experienced nor stockpiled the resources necessary for a hurricane of that magnitude. For example, Puerto Rico officials said their emergency plans allowed the local government to respond effectively to Hurricane Irma (e.g., evacuating residents, purchasing food, and securing their homes). However, their plans were insufficient for the magnitude of Hurricane María which made landfall two weeks later. Specifically, Puerto Rico officials had not considered that a hurricane would cause a loss of power for as long as Hurricane María did. [20]

In August 2018, eleven months after María Puerto Rico Electric Power Authority reported that power had been returned to all homes. By June 2018, Puerto Rican officials claimed that water service on the Island had been restored to more than 96 percent of customers. Service was restored to 96 percent of cell sites after only six months. María affected every resident on the Island, caused $90 billion in damages, and killed an estimated 4,645 people. [20] Maria was a full-scale Black Sky Event (BSE) that destroyed or critically impacted the electric grid, water infrastructure, telecommunications networks and nearly all other forms of modern society. The island's infrastructure was weak and vulnerable to storms well before Maria. But the government's efforts to respond were slow, insufficient, and lacking transparency. [25]

Part 2: Homeland Defense

Homeland Defense is the protection of US sovereignty, territory, domestic population, and critical infrastructure. Although Homeland Defense is a relatively new term that gained prominence following the attacks of September 11, 2001 (9/11), the concept is as old as the nation itself. Local militias were formed and trained to defend against Indian attacks starting with the first permanent English settlement of Jamestown in 1607. Colonial militia supported British regulars in the French and Indian War (1754-1763) to end raids along the frontier. The US Army was founded in 1775 to fight the British and help achieve independence in the Revolutionary War. President John Adams revived the US Navy in 1794 to protect US merchant ships on the Atlantic and Mediterranean seas. Although the US Army failed to stop the British from capturing and burning Washington DC in 1814, Major General Andrew Jackson's ramshackle force of regulars and volunteers routed the British at the Battle of New Orleans in 1815. In what some consider the longest war in US history, the American Indian Wars engaged the US Army from their inception in 1775 until the last Apache raid in 1924. Despite the Mexican War (1846-1848), Civil War (1861-1865), Spanish American War (1898), Mexican Border War (1910-1919)[1] and US involvement in World War I (1917-1918), after the War of 1812 US territorial integrity wasn't again seriously threatened by a foreign power until the Japanese attack on Pearl Harbor, December 7, 1941.

World War II

The attack on Pearl Harbor killed 2,403 Americans and damaged or destroyed 19 US Navy ships, including 8 battleships. The Japanese immediately followed up with further attacks against US bases in the Philippines, Guam, Midway, and Wake islands making them masters of the Pacific within a matter of days. Around the middle of December 1941, nine Japanese submarines arrived in American waters for the start of what was to be eight months of operations. Four of these boats eventually made attacks on coastal shipping, sinking two tankers and damaging one freighter. On 23 February 1942 the submarine I-17 surfaced near Santa Barbara and used its deck gun to fire thirteen 5.5-inch shells into oil installations, although with negligible damage. On the night of 21-22 June 1942, a submarine rose to the surface at the mouth of the Columbia River in Oregon and fired about a dozen 5.5-inch shells at Fort Stevens, a coast artillery fort. Militarily insignificant, that attack marked the first time since the War of 1812 that a foreign enemy had fired on a military installation in the continental United States. [26]

On December 11, 1941, three days after the US declared war against Japan, Hitler declared war on the US and sent his U-boats streaming into American waters. The first U-boats reached US waters on January 13, 1942. In the first three months of 1942, German U-boats sank more than 100 ships off the east coast of North America, the Gulf of Mexico, and the Caribbean Sea. Some sank within sight of land. Operation Drumbeat (January – June 1942) sank 397 ships totaling over 2 million tons. U-boat crews called it "the Second Happy Time".

[1] From the beginning of the Mexican Revolution in 1910, the United States Army was stationed in force along the border and, on several occasions, fought with Mexican rebels or federals. The height of the conflict came in 1916 when revolutionary Pancho Villa attacked the American border town of Columbus, New Mexico. In response, the United States Army, under the direction of General John J. Pershing, launched a "Punitive expedition" into northern Mexico, to find and capture Villa. Although Villa was not captured, the US Army found and engaged the Villista rebels, killing Villa's two top lieutenants. The revolutionary himself escaped and the American army returned to the United States in January 1917.

After the Munich Crisis in September 1938, the War Department determined that Germany and Japan were the principal threat to the United States. A year later, after England declared war on Germany, President Roosevelt and his military commanders began taking steps to prepare for a war many felt would inevitably involve the US. In 1940 the War Department began devising a series of "Rainbow" plans to meet the threat of a two-ocean war against multiple enemies.[2] RAINBOW 4 planned for defense of the United States without the aid of the United Kingdom or other European Allies. In May 1941, the Army created four strategic areas encompassing the continental United States designated as Eastern Defense Command, Western Defense Command, Southern Defense Command, and Central Defense Command. The Eastern and Western Defense Commands contained the majority of trained combat troops and aircraft squadrons. The Army also embarked on an ambitious plan to build 150 new coastal batteries fitted with 16-inch naval artillery and radar. [26]

It appeared in January 1942 that the defenses of the west coast had been breached by the attack on the US Pacific Fleet and the Hawaiian Islands. Two weeks of panic followed the Pearl Harbor attack as anxious citizens made many erroneous "sightings" of the Japanese fleet. The Army rushed antiaircraft units to defend the California oil industry; critical aircraft plants at Los Angeles, San Diego, and Seattle; and naval shipyards in the Puget Sound, in Portland, San Francisco, Los Angeles, and San Diego. By the end of February 1942 almost 250,000 troops had arrived to defend vital installations on the west coast, a task for which Army ground combat units were neither intended nor trained. General Marshall's chief concern was that the public fear of imminent invasion would freeze this force in a perimeter defense of the coast at a time when these regulars were desperately needed to train the citizen army being mobilized by the Selective Service System. [26]

After the Battle of Britain (July 1940 – May 1941) successfully fended off the threat of German invasion, the War Department began working on RAINBOW 5 which hypothesized sending American forces to fight in Europe and Africa. Planners understood that offensive action overseas would obviate the need for elaborate defenses at home. Within six months the demand for such defenses abated as Japanese intentions became clearer. If there had ever been a risk of west coast invasion, it disappeared after the Battles of Coral Sea (6-8 May 1942) and Midway (3-6 June 1942), which crippled the Japanese aircraft carrier force that would have been essential to an attack on the American mainland. After the results of Midway became clear, the Army began to stand down its defenses on the west coast, reassigning its Air Force units and antiaircraft forces to other duties. Thereafter, the War Department adopted a "calculated risk" policy that gave priority to mobilization duties rather than to passive defense. It was impossible for the Army both to garrison the long frontiers of the United States and to superintend the training of the mass Army needed to fight an offensive war. Offensive action had the clear priority, and almost immediately the manning of defensive garrisons began to take second place to the training needs of the Army. [26]

Unlike the American Navy, the Japanese never reconsidered submarine doctrine during the war. They continued to concentrate their submarines on attacking warships rather than merchantmen. The failure of Japanese submarines in the Pearl Harbor attack also apparently led Japanese naval commanders to discount their value. There was consequently no Japanese submarine plan that

[2] During the 1920s and 1930s, the United States Armed Forces developed a number of color-coded war plans that outlined potential US strategies for a variety of hypothetical war scenarios. The plans, developed by the Joint Planning Committee (which later became the Joint Chiefs of Staff) were officially withdrawn in 1939 at the outbreak of World War II in favor of five Rainbow Plans developed to meet the threat of a two-ocean war against multiple enemies.

paralleled the German offensive in the Atlantic or the enormously successful American campaign against the Japanese merchant fleet across the Pacific. As a result, American commerce on the west coast remained unmolested after the fall of 1942. Later Japanese attacks on the American mainland were limited to a series of incendiary attacks by free balloons, all of very limited consequence. [26]

German submarines enjoyed their greatest successes up until the middle of 1942. The US Navy gained the upper hand, however, after it acquired the resources and experience necessary to implement the convoy system, aerial patrols, and improved antisubmarine tactics to turn the tide in the Atlantic, Caribbean, and Gulf of Mexico. Army participation was chiefly in helping the Coast Guard patrol the beaches to forestall the landing of German agents. Equally important was the contribution made by the US ship industry which by 1943 could turn out three new merchant ships a day, faster than Germany could sink them. [26]

Unified Command Plan

Historical experience has taught that the most effective use of military force is through the combined application of air, land, and sea components to achieve unified action towards a common objective. This was a difficult lesson that with few exceptions eluded US military commanders for most of US history. Up until World War II the US military was organized and fought as a separate Army and Navy. In fact, the War Department was synonymous with the US Army because wars were generally considered to be won or lost on land. US Army generals pretty much viewed the purpose of the US Navy was to support land warfare (and some probably still do). The problem with this view was it promoted division and competition between the services that resulted in compromises in battle, some which led to disastrous losses. After the US entered World War II, the need to work together closely with our British allies made the necessity of unified action readily apparent. Thus, the US adopted the concept of “Unified Command” early on in the war. Unified command called for a single commander assisted by a Joint Staff to exercise direction and control over all military units within their assigned AOR, regardless of their service. The unified organization not only made more effective use of military force, it also provided a single point of contact for coordinating between nations. The system was generally applied during World War II in the conduct of individual operations and within geographic theater commands. One major exception was the US war in the Pacific. [27]

Instead of creating one unified command, the Pacific theater was divided into two. Having vowed “I shall return”, General Douglas Macarthur was given command over the Southern Pacific and mounted an “island hopping” campaign aimed at the Philippines. With the three aircraft carriers remaining after Pearl Harbor, Admiral Chester Nimitz was given command over the Central and Northern Pacific and mounted a strategic campaign aimed at Japan itself. [27]

The impetus for establishing a postwar system of unified command over US military forces worldwide stemmed from the Navy's dissatisfaction with this divided command in the Pacific. Following the war, the Chief of Naval Operations (CNO) characterized the arrangement as "ambiguous" and "unsatisfactory." He favored establishing a single command over the entire Pacific Theater (excluding Japan, Korea, and China), whose commander would have a joint staff and would exercise "unity of command" over all US forces in the theater. After considerable discussion, a compromise emerged as part of a comprehensive worldwide system of unified command for US forces. The resulting “Outline Command Plan” signed by President Truman in December 1946 became the first Unified Command Plan (UCP) for the operational direction and control of US military forces. The first UCP established eight Geographic Combatant Commands:

1. **Far East Command**. The Commander in Chief (CINC) of Far East Command (CINCFE) would have direction and control over US forces in Japan, Korea, the Ryukyus, the Philippines, the Marianas, and the Bonins. CINCFE would carry out occupation duties, maintain the security of his command, plan and prepare for a general emergency in his area, support CINCPAC, and command US forces in China in an emergency.
2. **Pacific Command**. CINCPAC was given direction and control over US military forces allocated by the Joint Chiefs of Staff (JCS) within the Pacific area. CINCPAC would defend the US against attack through the Pacific, conduct operations in the Pacific, and maintain security of US island positions and sea and air communications, support US military commitments in China, plan and prepare for general emergency, and support CINCFE and CINCAL.
3. **Alaskan Command**. CINCAL had direction and control of US forces in Alaska, including the Aleutians. CINCAL would protect Alaska, including sea and air communications, and protect the United States from attack through Alaska and the Arctic regions. He would plan and prepare for general emergency and support CINCFE, CINCPAC, and the Commanding General (CG) of Strategic Air Command (SAC).
4. **Northeast Command**. CINCNE had direction and control of US forces assigned to Newfoundland, Labrador, and Greenland. CINCNE would maintain the security of his area and defend the United States against attack through the Arctic regions within his command; protect sea and air communications in his area; control Arctic airways as appropriate; support CINCEUR, CINCLANTFLT and SAC; and plan and prepare for a general emergency.
5. **Atlantic Fleet**. CINCLANTFLT had direction and control over the US Atlantic Fleet. CINCLANTFLT would defend the United States against attack through the Atlantic; plan and prepare for general emergency; and support US forces in Europe, the Mediterranean, the Northeast, and the Caribbean.
6. **Caribbean Command**. CINCARIB was given direction and control over US forces in Panama and the Antilles. CINCARIB would defend the United States against attack through his area; defend sea and air communications (with CNO coordinating between CINCARIB and CINCLANTFLT); secure the Panama Canal and US bases in Panama and the Caribbean; plan and prepare for general emergency; and support CINCLANTFLT.
7. **European Command**. CINCEUR had direction and control over all forces allocated to the European Theater by the JCS or other authority. CINCEUR would occupy Germany, support the national policy in Europe "within the scope of his command responsibility," and plan and prepare for general emergency. [27]

Of the eight Geographic Combatant Commands created in the first UCP, only two, Far East Command and European Command, didn't have direct responsibility for defending the US mainland.

Although the concept was sound, the development of unified commands was imperfect due to continuing inter-service rivalry and underwent evolutionary change due to new and emerging threats.

Cold War

World War II was ended by the atomic bombing of Hiroshima and Nagasaki. It is estimated that 66,000 were killed and 69,000 injured in Hiroshima, plus 39,000 killed and 25,000 injured in Nagasaki.[3]

[3] There has been great difficulty in estimating the total casualties in the Japanese cities as a result of the atomic bombing. The extensive destruction of civil installations (hospitals, fire and police department, and government

Although German cities were equally decimated by Allied bombing, the stark difference between the two campaigns is evident in the numbers: Allied air forces in Europe dropped nearly 2.7 million tons of bombs, flew 1,440,000 bomber sorties and 2,680,000 fighter sorties, lost 40,000 aircraft and 160,000 aircrew; by comparison, fourteen aircrew from the 509th Composite Group flew two B-29s on two missions that dropped two bombs. Japan's surrender on September 2, 1945 resulted in the cancellation of Operation Downfall, the planned invasion of the Japanese home islands scheduled for that November. As horrific as the casualties were from the atomic bombings, they paled in comparison to the estimated fatalities for Operation Downfall: 500,000 Americans, 5-10 million Japanese.[4]

The United States emerged from World War II with a monopoly on atomic weapons. This was deemed important to counter the massive imbalance of power and growing wariness between East and West on the former battlefields of Europe. After the war, relations between the US and its former ally the Soviet Union quickly deteriorated as Stalin sought to impress communism upon those territories his forces occupied. The Cold War began March 12, 1947 when the American policy of Soviet containment was formalized in the Truman Doctrine. Although the doctrine sought to avoid direct military confrontation, the US monopoly on atomic weapons gave it a strategic advantage against the numerically superior Soviet conventional forces. It was this US atomic advantage that perhaps prevented the numerically superior Soviet Union from overrunning the allies and instead implementing a blockade that precipitated the 1948-49 Berlin Airlift. The US advantage ended when the Soviet Union successfully tested its own atomic bomb in August 1949. With it came the prospect of direct Soviet attack on the US should the Cold War turn hot.

Following the successful detonation of its first atomic bomb in August 1949, the Soviet Union aggressively pursued the acquisition of more and mightier weapons and the means to deliver them to the US. In November 1952, the USSR first flew the Tupolev Tu-95 (NATO call sign "Bear") bomber with a range of 5,000 miles capable of dropping an atomic bomb on the US. In November 1955, the Soviet Union detonated its first hydrogen bomb yielding 1.6 megatons of explosive force, more than 100 times that which destroyed Hiroshima Japan during World War II. And in October 1957 the USSR launched Sputnik 1, the first artificial Earth satellite carried into orbit atop a modified R-7 intercontinental ballistic missile.

US Air Defense

By 1954 the increasing threat of Soviet atomic air attack on the continental United States led the JCS to establish a new unified command to defend against this new danger. The Continental Air Defense Command (CONAD) was established September 1, 1954 to coordinate air defense for the continental United States. Headquartered at Ent Air Force Base in Colorado Springs, CONAD was given direction and

---

agencies) the state of utter confusion immediately following the explosion, as well as the uncertainty regarding the actual population before the bombing, contribute to the difficulty of making estimates of casualties. The Japanese periodic censuses are not complete. Finally, the great fires that raged in each city totally consumed many bodies. The number of total casualties has been estimated at various times since the bombings with wide discrepancies. These numbers represent the best available estimate from the Manhattan Engineer District which built the bombs.

[4] Because they are often cited as justification for the atomic bombings, the estimated casualties for Operation Downfall are hotly debated today as they were in 1945. The Japanese fought more fiercely the nearer the fighting came to their home islands. The Battle of Okinawa was the bloodiest killing 14,009 Allies and 77,417 Japanese. If the casualty rate for Operation Downfall was only 5% that in Okinawa, losses would still be catastrophic at 300,000 Americans and 1.6 million Japanese. The figures cited in this report were estimated by William Shockley, on staff with Secretary of War Henry L. Stimson.

control over service elements assigned to US Air Force Air Defense Command, the US Army Antiaircraft Command, and the US Navy Contiguous Coverage Radar System. [27] Air Defense Command maintained ready and alert fighter interceptors and surface-to-air missiles (SAMs) across the continental US, Alaska, Canada, and Greenland. Army Antiaircraft Command maintained surface-to-air missile batteries at various locations around the US. The Army Nike-Ajax was the first operational SAM deployed in the US. It was soon superseded by the Nike-Hercules which carried a W31 two kiloton nuclear warhead. The Air Force BOMARC surface-to-air missile carried a W40 ten kiloton nuclear warhead. Both the Nike-Hercules and BOMARC missiles were designed to destroy large formations of Soviet bombers attacking the US. The Contiguous Radar Coverage System consisted of land-based radars across the width of southern Canada called the "Pinetree Line", and "Seaward Extensions" in the Atlantic and Pacific Oceans. The Navy Seaward Extensions included airborne early warning aircraft and two radar platforms off the US northeast coast. The system could detect enemy bombers out to a distance of 400 to 500 miles providing about 45 to 55 minutes warning of attack.

Upon gaining office in 1953, President Eisenhower ordered a review of US military strategy with the aim of balancing Cold War commitments against the nation's financial resources. The resulting "New Look" national security policy emphasized reliance on strategic nuclear weapons to deter potential Soviet aggression. To maintain a credible deterrence, it was essential that US nuclear bombers not get caught on the ground in a Soviet attack. An ironic consequence of the New Look policy was that the major objective of continental air defense was to buy time for US bombers to launch; shooting down Soviet bombers became a secondary concern.

In September 1957 a combined US-Canadian command, the North American Air Defense Command (NORAD) was established to defend the Continental United States, Canada, and Alaska against air attack. Both US and Canada air defense commands were merged together in a single headquarters at Ent Air Force Base in Colorado Springs. By agreement, CINCONAD also became CINCNORAD. As senior US officer in NORAD headquarters, CINCONAD was given operational control over assigned US forces to defend US installations in Greenland against air attack; assist in the defense of Canada and Mexico; and maintain air defense of the continental United States and Alaska. Also by agreement, NORAD's first priority was to provide sufficient warning and defense to buy time for US bombers to launch. After Sputnik, this presented a bit of a problem. [27]

In March 1957, an adequate and timely defense system against intercontinental ballistic missiles became "the most urgent future CONAD requirement." The same held true for cruise missiles and ballistic missiles launched from Soviet submarines or warships. On June 14, 1957 The Gaither Report, a presidentially commissioned review of US nuclear policies noted "little likelihood of [US] bombers surviving since there was no way to detect an incoming attack until the first [ICBM] warhead landed".

Bridging the Missile Gap

On October 4, 1957 the successful Soviet launch of Sputnik, the world's first artificial satellite came as a shock to both experts and the general public in the United States. The fact that the Soviets were successful fed fears that the US military had generally fallen behind in developing new technology. As a result, the launch of Sputnik served to intensify the arms race and raise Cold War tensions.

During the 1950s, both the United States and the Soviet Union were working to develop new technology. Nazi Germany had been close to developing the world's first intercontinental ballistic missile (ICBM) near the end of the Second World War, and German scientists aided research in both countries in the wake of that conflict. Both countries were also engaged in developing satellites as a part of a goal

set by the International Council of Scientific Unions, which had called for the launch of satellite technology during late 1957 or 1958. Over the course of the decade, the United States tested several varieties of rockets and missiles, but all of these tests ended in failure.

The success of Sputnik had a major impact on the Cold War and the United States. Fear that they had fallen behind led US policymakers to accelerate space and weapons programs. In the late 1950s, Soviet Premier Nikita Khrushchev boasted about Soviet technological superiority and growing stockpiles of ICBMs, so the United States worked simultaneously to develop its own ICBMs to counter what it assumed was a growing stockpile of Soviet missiles directed against the United States. With both countries researching new technology, talk of creating a treaty banning nuclear testing faded away for several years. In this way, the launch of Sputnik fueled both the space race and the arms race, in addition to increasing Cold War tensions, as each country worked to prepare new methods of attacking the other. Eventually, lawmakers and political campaigners in the United States successfully exploited the fear of a "missile gap" developing between US and Soviet nuclear arsenals in the 1960 presidential election, which brought John F. Kennedy to power over Eisenhower's vice president, Richard Nixon. [28]

Strategic Nuclear Triad

Since the early 1960s the United States has maintained a "triad" of strategic nuclear delivery vehicles. These include land-based ICBMs, submarine-launched ballistic missiles (SLBMs), and long-range heavy bombers.

The Air Force ballistic missile program had its origins in studies and projects initiated by the Army Air Corps immediately after World War II. These efforts aimed at mating the German V-2 ballistic missile and the atomic bomb, a union that carried the potential for a revolution in strategic warfare. Technical problems held the program back at first, but the situation was changed drastically by the so-called "thermonuclear breakthrough" of the early 1950's. This breakthrough made it possible to manufacture high-yield nuclear weapons that were small enough and light enough to be carried as warheads aboard ballistic missiles.

The Air Force was in the middle of developing both the Atlas and Titan ICBMs when Sputnik launched in October 1957. In January 1951 the Air Force contracted with the Convair Corporation to develop the Atlas. Weighing 267,000 pounds and standing 82 feet tall, the two-stage Atlas ICBM had an approximate range of 6,500 miles and could deliver a 1-megaton thermonuclear warhead within one-and-a-half miles of its target. Atlas became the first US operational ICBM in October 1959. However, there were drawbacks. The liquid-fueled Atlas was stored above-ground, making it vulnerable to attack, and took a long time to launch. Recognizing these shortcomings, the Air Force in 1954 contracted with Martin Aircraft Company to develop the Titan. Standing 98 feet tall, the Titan I had the same approximate range as the Atlas but could deliver twice the payload. Moreover, the Titan I could be stored underground, making it more protected, but it still had to be raised for launch, still making it slow. The first Titan I squadron was activated in April 1960 at Lowery Air Force Base in Colorado.

Both the liquid-fueled Atlas and Titan ICBMs were expensive to maintain, difficult to deploy, and dangerous to operate. In September 1959 the Air Force contracted with the Boeing Airplane Company to develop the Minuteman. The Minuteman employed a solid booster rocket allowing it to be quickly launched from its protected underground silo. The first Minuteman I squadron was activated July 1962 at Malmstrom Air Force Base in Montana. The Minuteman II entered service in 1965 with a host of upgrades to improve its accuracy and survivability in the face of an anti-ballistic missile (ABM) system the Soviets were known to be developing. In 1970, the Minuteman III became the first deployed ICBM

with multiple independently targetable reentry vehicles (MIRV): three smaller warheads that improved the missile's ability to strike targets defended by ABMs. By the 1970s, over 1,000 Minuteman missile were deployed across the US. [29]

In the mid-1950s the Navy was involved in the Jupiter missile project with the US Army and had influenced the design by making it squat so it would fit in submarines. However, they had concerns about the use of liquid fuel rockets on board ships, and some consideration was given to a solid fuel version, the Jupiter S. In 1956, during an anti-submarine study known as Project Nobska, the famous physicist Edward Teller suggested that very small hydrogen bomb warheads were possible. A crash program to develop a missile suitable for carrying such warheads began as Polaris. The first Polaris missile successfully launched less than four years later, in February 1960. Polaris formed the backbone of the US Navy's nuclear force aboard a number of custom-designed submarines. Beginning in 1972 the Polaris missile was replaced by the MIRV-capable Poseidon missile. During the 1980s, these missiles were replaced by the Trident I missile. In 1981 the US Navy commissioned the USS Ohio ballistic missile submarine (SSBN) capable of carrying 20 Trident missiles each carrying three warheads. Over the next twenty years it launched 14 Ohio-class SSBNs.

The SLBM held several advantages over the land-based ICBM. First, it could be launched closer to enemy territory providing a quicker strike capability. Second, whereas ICBM positions were fixed and known, the positions of SLBMs carried aboard ballistic missile submarines were dynamic and unknown. These advantages led the Navy to suggest, starting around 1959, that they be given the entire nuclear deterrent role. This led to new infighting between the Navy and the US Air Force, the latter responding by developing the counterforce concept that argued for the strategic bomber and ICBM as key elements in flexible response. [30]

Although nuclear missiles could strike faster and not be stopped, nuclear bombers still retained one key advantage; they could be recalled. The B-29 Superfortress that dropped the atomic bombs on Hiroshima and Nagasaki in World War II had a maximum cruising speed of 217 mph, 33,000 ft. ceiling, 12,000 lb. payload, and 1,600 mile range. It quickly became apparent at the outset of the Cold War that the B-29 was ill-equipped to strike targets deep inside the Soviet Union. In 1948 the Air Force took delivery of the B-36 Peacemaker. The B-36 was a massive aircraft twice the size of the B-29 capable of carrying six times the payload over six times the distance. Unfortunately, its six rear-facing piston engines gave it a cruising speed of 230 mph making it vulnerable to jet fighter interceptors. In 1955 the Air Force took delivery of the B-52 Stratofortress. Powered by six jet engines, the B-52 had the range and payload of the B-29, but with a 50,000 ft. ceiling and 300 mph cruising speed, it could fly twice as high and twice as fast as the B-29. In 1960 the B-58 Hustler entered service as the first supersonic bomber. The B-58 had a ceiling of 63,000 ft. and was capable of achieving Mach 2. It was also very expensive and difficult to maintain, which is why it was retired after only ten years of service. By the 1970s, sophisticated Soviet radars and surface-to-air missiles made the tactic of high-altitude bombing that had prevailed since World War II no longer tenable. To reach targets deep inside the USSR, Air Force bombers would have to fly close to the ground below Soviet radar. The B-52 was upgraded with terrain-following radar, sophisticated navigation and electronic countermeasures to help it penetrate Soviet air defenses, but the aircraft was getting old. The B-1 Lancer was designed in the 1960s to replace the B-58 Hustler, and after a cancellation delay in the 1970s, finally entered Air Force service as the B-1b in 1986. The swing-wing B-1B has the same 75,000 lb. payload capacity as the B-52, but can cruise at high subsonic speeds with sustained supersonic sprints. Although capable of carrying a nuclear payload, the B-1b is not part of the Air Force’s nuclear fleet. The reason for this, and the reason for the delay to

the B-1b was the introduction in 1993 of the B-2 Spirit stealth bomber. Built by Northrop Grumman, the B-2 flying wing can deliver a 38,000 payload 6,000 miles into heavily defended airspace. The 20 B-2s comprising the 13th Bomb Squadron at Whiteman Air Force Base Missouri are part of the same 509th Operations Group that dropped the first atomic bombs during World War II.

The United States developed these three different types of nuclear delivery vehicles, in large part, because each of the military services wanted to play a role in the US nuclear arsenal. However, during the 1960s and 1970s, analysts developed a more reasoned rationale for the nuclear "triad." They argued that these different basing modes would enhance deterrence and discourage a Soviet first strike because they complicated Soviet attack planning and ensured the survivability of a significant portion of the US force in the event of a Soviet first strike. The different characteristics of each weapon system might also strengthen the credibility of US targeting strategy. To be specific, ICBMs have the accuracy and prompt responsiveness needed to attack hardened targets such as Soviet command posts and ICBM silos, SLBMs have the survivability needed to complicate Soviet efforts to launch a disarming first strike and to retaliate if such an attack were attempted, and heavy bombers can be dispersed quickly and launched to enhance their survivability, and they can be recalled to their bases if a crisis did not escalate into conflict. [31]

Anti-Ballistic Missile Defense

Following World War II, the US Army began planning for research and development of missile defenses. The first known serious study on attacking ballistic missiles with interceptor missiles was carried out by the Army Air Force in 1946, when two contracts were sent out as Project Wizard and Project Thumper to consider the problem of shooting down missiles of the V-2 type. These projects identified the main problem being one of detection; the target could approach from anywhere within hundreds of miles, and reach their targets in only five minutes. Existing radar systems would have difficulty seeing the missile launch at those ranges, and even assuming one had detected the missile, existing command and control arrangements would have serious problems forwarding that information to the battery in time for them to attack. The task appeared impossible at that time.

After Sputnik, President Eisenhower began the search for a defense to ballistic missiles when he authorized the operational development of a nuclear-tipped interceptor missile, Nike-Zeus, and commissioned Project Defender to develop components for a nationwide ballistic missile defense system. The original, Zeus A, was designed to intercept warheads in the upper atmosphere, mounting a 25 kiloton W31 nuclear warhead. During development, the concept changed to protect a much larger area and intercept the warheads at higher altitudes. This required the missile to be greatly enlarged into the totally new design, Zeus B, given the tri-service identifier XLIM-49, mounting a 400 kiloton W50 warhead. In several successful tests, the B model proved itself able to intercept warheads, and even satellites.

While Nike-Zeus was under development, the nature of the threat changed dramatically and dramatically changed the course of development. Originally expected to face only a few dozen Soviet ICBMs, a nationwide defense was feasible, although expensive. But when the Soviets claimed to be building hundreds of missiles, the US faced the problem of building enough Zeus missiles to match them. The Air Force argued they close this missile gap by building more ICBMs of their own instead. Adding to the debate, a number of technical problems emerged that suggested Zeus would have little capability against any sort of sophisticated attack. The decision whether to proceed with Zeus eventually fell to President John F. Kennedy, who became fascinated by the debate about the system. In 1963, the United

States Secretary of Defense, Robert McNamara, convinced Kennedy to cancel Zeus. McNamara directed its funding towards an experimental Nike-X program and studies of anti-ballistic missile (ABM) concepts being considered by the Pentagon's newly created Advanced Research Projects Agency (ARPA). [32]

ARPA began tackling the problems that plagued Nike-Zeus. The first was the limited ability of radars to track multiple targets. The 1957 Gaither Committee report suggested radar limitations gave a salvo of only four warheads a 90% chance of destroying a Zeus base. Another problem was high-altitude nuclear explosions. They tended to blanket a large area with radiation that blocked radar signals above 37 miles altitude. By exploding a single warhead above a Zeus site, the Soviets could block radar observation until the following warheads were too close to attack. Finally, there was the problem of decoys. By simply packing radar reflectors into the missile, they would present many false targets that would be indistinguishable from the real warhead.

After analyzing these problems, ARPA noted that both the radar decoys and high-altitude explosions stopped working in the thickening lower atmosphere. If one simply waited until the warheads descended below about 60 km, they could be easily picked out on radar again. However, as the warheads would be moving at about 5 miles per second (8 km/s; Mach 24) at this point, they were only seconds from their targets. An extremely high-speed missile would be needed to attack them during this period.

In response, Martin Marietta developed the Spring missile. It was a two-stage solid-fuel anti-ballistic missile armed with a W66 2-kiloton nuclear warhead. Sprint accelerated at 100 g, reaching a speed of Mach 10 in 5 seconds. Such a high velocity at relatively low altitudes created skin temperatures up to 6,200 °F, requiring an ablative shield to dissipate the heat. The high temperature caused a plasma to form around the missile, requiring extremely powerful radio signals to reach it for guidance. The missile glowed bright white as it flew. [33]

Sprint was the centerpiece of the Nike-X system. The key concept that led to Nike-X was that the rapidly thickening atmosphere below 37 miles altitude disrupted the reflectors and explosions. Nike-X intended to wait until the enemy warheads descended below this altitude and then attack them using the very fast Sprint missile. The entire engagement would last only a few seconds and could take place as low as 25,000 feet. To provide the needed speed and accuracy, as well as deal with multi-warhead attacks, Nike-X used a new radar system that could track hundreds of objects at once and control salvos of many Sprints.

Nike-X depended on phased-array radar to track multiple incoming warheads and guide the Sprint missiles targeted against them. Phased-array radar generated multiple virtual radar beams, simulating any number of mechanical radars needed. While one beam scanned the sky for new targets, others were formed to examine the threat tubes and generate high-quality tracking information very early in the engagement. More beams were formed to track warhead re-entry vehicles (RVs) once they had been picked out, and still more to track the Sprints on their way to the interceptions. To make all of this work, the phased-array radar required data processing capabilities on an unprecedented scale and was an early adopter of new integrated circuit technology.

Because the Sprint was designed to operate at short range, a single base could not provide protection to a typical US city, given urban sprawl. This required the Sprint launchers to be distributed around the defended area. Most nationwide deployment scenarios contained thousands of Sprint missiles protecting only the largest US cities. Such a system would cost an estimated $40 billion to build, about half the military budget at the time.

This led to further studies of the Nike-X to try to determine whether an ABM would be the proper way to save lives, or if there was some other plan that would do the same for less money. **In the case of Nike-Zeus, for instance, it was clear that building more fallout shelters would be less expensive and save more lives. A major report on the topic by President's Science Advisory Committee in October 1961 made this point, suggesting that Zeus without shelters was useless, and that having Zeus might lead the US to "introduce dangerously misleading assumptions concerning the ability of the US to protect its cities".**

Deployment options for Nike-X boiled down to four choices: 1) Heavy Defense, 2) Nth Country "Thin Defense", 3) Hardsite, and 4) I-67. The Heavy Defense option would deploy Nike-X near major US cities for $40 billion while affording only limited protection. The Nth Country option would deploy Nike-X to a few strategic sites around the country to protect against a limited nuclear attack at a cost of $5 billion while affording no protection under certain scenarios. Hardsite would deploy Nike-X near Minuteman missile fields for about the same cost as Nth Country while affording some protection against a certain class of counterforce attacks. I-67 was essentially Nth Country but with more bases near Minuteman fields.

None of the proposed Nike-X deployment concepts appeared to be particularly worthwhile, but there was considerable pressure from Congressional groups dominated by hawks who continued to force development of the ABM even when Secretary McNamara and President Johnson had not asked for it. Pressure only mounted when the Soviet Union began building its own A-35 ABM system around Moscow and Tallinn. In December 1966, McNamara proposed that the money sidelined by Congress for deployment be used for initial deployment studies while the US attempted to negotiate an arms limitation treaty. Johnson agreed with this compromise and ordered Secretary of State Dean Rusk to open negotiations with the Soviets. In June 1967 the Chinese tested their first H-bomb. Suddenly the Nth Country concept was no longer simply theoretical. On September 18, 1967, Secretary McNamara renamed Nike-X Sentinel and outlined deployment plans broadly following the I-67 concept. [34]

Sentinel would have seventeen bases, each centered on a Missile Site Radar (MSR) with a computerized command center buried below it. The system was supported by a string of five long-range Perimeter Acquisition Radars (PAR) spread across the US/Canada border area and another in Alaska. The primary weapon was the long-range Spartan missile, with short range Sprint missiles providing additional protection near US ICBM fields and PAR sites. The system would initially have a total of 480 Spartan and 192 Sprint missiles. Construction of the first Sentinel base began outside Bostin in 1968.

By the time Richard Nixon took office in January 1969, public opinion had swung strongly against ABMs. Residents of the cities to be protected protested that it simply made them targets for more Soviet bombs, and there were a number of well organized public demonstrations against the Sentinel system. Nixon ordered a review that suggested sweeping changes to the system, and the Sentinel program was cancelled in March 1969 after only 18 months of existence. In its place, an even lighter system intended primarily to defend USAF missile bases was introduced, the Safeguard Program. [35]

The Safeguard Program was a US Army ABM system designed to protect the US Air Force's Minuteman ICBM silos from attack, thus preserving the US's nuclear deterrent capability. It was intended primarily to protect against the very small Chinese ICBM fleet, limited Soviet attacks and various other limited-launch scenarios. A full-scale attack by the Soviets would easily overwhelm it. Similar in composition to the Sentinel system, Safeguard was originally planned for deployment to Whiteman AFB, Missouri, Malmstrom AFB, Montana, and Grand Forks AFB, North Dakota.

Meanwhile, arms limitation talks between the US and Soviet Union started by President Johnson finally bore fruit under the Nixon Administration in the form of the 1972 Anti-Ballistic Missile Treaty. The ABM Treaty limited the US and Soviet Union to two ABM sites each. Safeguard was consequently scaled back to sites in North Dakota and Montana, and work at the site in Missouri abandoned. Construction on the two remaining bases continued until 1974, when an additional agreement limited both countries to a single ABM site. The Montana site was abandoned with the main radar partially completed. The remaining base in North Dakota, the Stanley R. Mickelsen Safeguard Complex, became active on April 1, 1975 and fully operational October 1, 1975. By that time the House Appropriations Committee had already voted to deactivate it. The base was shut down on 10 February 1976. [36]

Strategic Defense Initiative

Following closure of the Safeguard ABM site in 1976, the US had no defensive capability against Soviet nuclear missiles and relied solely on nuclear deterrence to avert World War III. President Reagan was a vocal critic of the doctrine of mutually assured destruction (MAD) which he described as a "suicide pact". After discussing options with Edward Teller, on March 23, 1983 President Reagan called on American scientists and engineers to develop a system that would render nuclear weapons obsolete. The Strategic Defense Initiative revived the concept of a missile defense system intended to protect the US from attack by ballistic nuclear missiles. Critics derisively nicknamed it "Star Wars".

In 1984 the Strategic Defense Initiative Organization (SDIO) was set up in within the US Department of Defense to oversee development. A wide array of advanced weapon concepts, including lasers, particle beam weapons and ground- and space-based missile systems were studied, along with various sensor, command and control, and high-performance computer systems that would be needed to control a system consisting of hundreds of combat centers and satellites spanning the entire globe. SDIO predominantly invested in basic research at national laboratories, universities, and in industry.

In 1987, the American Physical Society (APS) concluded that the technologies being considered were decades away from being ready for use, and at least another decade of research was required to know whether such a system was even possible. After the publication of the APS report, SDI's budget was repeatedly cut. By the late 1980s, the effort had been re-focused on the "Brilliant Pebbles" concept using small orbiting missiles not unlike a conventional air-to-air missile, which was expected to be much less expensive to develop and deploy. [37]

SDI was ultimately most effective not as an anti-ballistic missile defense system, but as a propaganda tool which put military and economic pressure on the Soviet Union to fund their own anti-ballistic missile system. This possibility was particularly significant because, during the 1980s, the Soviet economy was teetering on the brink of disaster. "Why can't we just lean on the Soviets until they go broke?" quipped Reagan. Although Reagan was sincerely invested in SDI for the purposes of national security and never intended for it to be a bargaining chip, many of his advisors acknowledged its potential as a negotiating tool. Despite his concerns about the shortcomings of SDI as a legitimate system of defense, Shultz recalled saying at the time, "The Soviets will assume that we are on the verge of some special technical innovation. Maybe that is the greatest benefit" Shultz's assessment proved to be correct. As Soviet Ambassador Dobrynin explained, the Soviet Union believed "that the great technological potential of the United States had scored again and treated Reagan's statement as a real threat". Soviet scientists were immediately tasked with investigating SDI. Physicist Roald Sagdeev, who was a part of this effort, recalled, "You know what the major argument was for investigating? What we were most afraid of? We were afraid that the industrialists in our military-industrial complex would say,

‘Great, we should do the same thing’”. Sagdeev later acknowledged, “If Americans oversold [SDI], we Russians overbought it.” [38]

Informed opinion suggests that SDI did not end the Cold War, but the Cold War did end SDI. If the Cold War started March 12, 1947 when President Truman made an address to Congress announcing his doctrine to contain communism, the Cold War ended when the Soviet Union collapsed on December 26, 1991. The rapid and unexpected dissolution brought a wave of relief that the nightmare was over and the nation was no longer held hostage by a nuclear Sword of Damocles. It also raised expectations of a “peace dividend” in anticipation of major cutbacks to military programs. The end of the Cold War and the rapid reduction of nuclear arsenals on both side undermined political support for SDI. SDI officially ended in 1993, when the Clinton Administration redirected the efforts towards theatre ballistic missiles and renamed the agency the Ballistic Missile Defense Organization (BMDO). [37]

Nuclear Close Calls

US deterrence policy depends on rational leaders making rational decisions under extreme conditions with little room for error. Historical incidents demonstrate that accidents, miscalculations, and plain luck have both brought the nation to the brink of nuclear holocaust and saved it from it.

5 Nov 1956, Suez Crisis

During the Suez Crisis, the North American Aerospace Defense Command received a number of simultaneous reports, including unidentified aircraft over Turkey, Soviet MiG-15 fighters over Syria, a downed British Canberra medium bomber, and unexpected maneuvers by the Soviet Black Sea Fleet through the Dardanelles that appeared to signal a Soviet offensive. Considering previous Soviet threats to use conventional missiles against France and the United Kingdom, U.S. forces believed these events could trigger a NATO nuclear strike against the Soviet Union. In fact, all reports of Soviet action turned out to be erroneous, misinterpreted, or exaggerated. The perceived threat was due to a coincidental combination of events, including a wedge of swans over Turkey, a fighter escort for Syrian President Shukri al-Quwatli returning from Moscow, a British bomber brought down by mechanical issues, and scheduled exercises of the Soviet fleet.

Aug – Dec 1958, Second Taiwan Crisis

US Secretary of State Christian Herter characterized the Second Taiwan Strait Crisis as "the first serious nuclear crisis". In this conflict, the PRC shelled the islands of Kinmen (Quemoy) and the Matsu Islands along the east coast of mainland China (in the Taiwan Strait) to "liberate" Taiwan from the Chinese Nationalist Party, also known as the Kuomintang (KMT); and to probe the extent of the United States defense of Taiwan's territory. A naval battle also took place around Dongding Island when the ROC Navy repelled an attempted amphibious landing by the PRC Navy.

5 Oct 1960, Greenland Moonrise Incident

Radar equipment in Thule, Greenland, mistakenly interpreted a moonrise over Norway as a large-scale Soviet missile launch. Upon receiving a report of the supposed attack, NORAD went on high alert. However, doubts about the authenticity of the attack arose due to the presence of Soviet leader Nikita Khrushchev in New York City as head of the USSR's United Nations delegation.

24 Jan 1961, Goldsboro Broken Arrow

On 24 January 1961, a B-52 Stratofortress carrying two 3–4-megaton Mark 39 nuclear bombs broke up in mid-air near Goldsboro, North Carolina, dropping its nuclear payload in the process. The pilot in command, Walter Scott Tulloch, ordered the crew to eject at 9,000 feet. Five crewmen successfully ejected or bailed out of the aircraft and landed safely, another ejected but did not survive the landing, and two died in the crash. Information declassified in 2013 showed that "only a single switch prevented the ... bomb from detonating and spreading fire and destruction over a wide area." An expert evaluation written on 22 October 1969 by Parker F. Jones, the supervisor of the nuclear weapons safety department at Sandia National Laboratories, reported that "one simple, dynamo-technology, low voltage switch stood between the United States and a major catastrophe", and that it "seems credible" that a short circuit in the Arm line during a mid-air breakup of the aircraft "could" have resulted in a nuclear explosion."

24 Nov 1961, BMEWS Blackout Incident

Staff at the Strategic Air Command Headquarters (SAC HQ) simultaneously lost contact with NORAD and multiple Ballistic Missile Early Warning System sites. Since these communication lines were designed to be redundant and independent from one another, the communications failure was interpreted as either a very unlikely coincidence or a coordinated attack. SAC HQ prepared the entire ready force for takeoff before already-overhead aircraft confirmed that there did not appear to be an attack. It was later found that the failure of a single relay station in Colorado was the sole cause of the communications problem.

25 Oct 1962, Cuban Missile Crisis – Bear Alert

During the Cuban Missile Crisis, US military planners expected that sabotage operations might precede any nuclear first strike by the Soviet Union. Around midnight on 25 October 1962, a guard at the Duluth Sector Direction Center saw a figure climbing the security fence. He shot at it and activated the sabotage alarm, which automatically set off similar alarms at other bases in the region. At Volk Field in Wisconsin, a faulty alarm system caused the Klaxon to sound instead, which ordered Air Defense Command nuclear-armed F-106A interceptors into the air. The pilots had been told there would be no practice alert drills and, according to political scientist Scott D. Sagan, "fully believed that a nuclear war was starting". Before the planes were able to take off, the base commander contacted Duluth and learned of the error. An officer in the command center drove his car onto the runway, flashing his lights and signaling to the aircraft to stop. The intruder was discovered to be a bear. Sagan writes that the incident raised the dangerous possibility of an ADC interceptor accidentally shooting down a Strategic Air Command bomber. Interceptor crews had not been given full information by SAC of plans to move bombers to dispersal bases (such as Volk Field) or the classified routes flown by bombers on continuous alert as part of Operation Chrome Dome. Declassified ADC documents later revealed that "the incident led to changes in the alert Klaxon system [...] to prevent a recurrence".

27 Oct 1962, Cuban Missile Crisis – B-59 Submarine Incident

At the height of the Cuban Missile Crisis, Soviet patrol submarine B-59 almost launched a nuclear-armed torpedo while under harassment by American naval forces. One of several vessels surrounded by American destroyers near Cuba, B-59 dove to avoid detection and was unable to communicate with Moscow for a number of days. USS Beale began dropping practice depth charges to signal B-59 to surface; however the captain of the Soviet submarine and its zampolit took these to be

real depth charges. With low batteries affecting the submarine's life support systems and unable to make contact with Moscow, the commander of B-59 feared that war had already begun and ordered the use of a 10-kiloton nuclear torpedo against the American fleet. The zampolit agreed, but the chief of staff of the flotilla (second in command of the flotilla) Vasily Arkhipov refused permission to launch. He convinced the captain to calm down, surface, and make contact with Moscow for new orders.

27 Oct 1962, Cuban Missile Crisis – U-2 Incident

On the same day as the B-59 was about to launch a nuclear torpedo, an American U-2 spy plane was shot down over Cuba, and another U-2 flown by United States Air Force Captain Charles Maultsby from Eielson Air Force Base, Alaska, strayed 300 miles into Soviet airspace. Despite orders to avoid Soviet airspace by at least 100 miles, a navigational error caused by the aurora borealis took the U-2 over the Chukotka Peninsula, causing Soviet MiG interceptors to scramble and pursue the aircraft. American F-102A interceptors armed with GAR-11 Falcon nuclear air-to-air missiles (each with a 0.25 kiloton yield) were then scrambled to escort the U-2 into friendly airspace. Individual pilots were capable of arming and launching their missiles. The incident remained secret for many years.

28 Oct 1962, Cuban Missile Crisis – Kadena Launch Order

Before dawn a mistaken order was issued by Kadena Air Base in Okinawa to nuclear missile sites in Okinawa to launch all their nuclear missiles. None was launched. A team responsible for four missiles at Bolo Airfield in Yomitan reported that the order's codes were in order, but the local officer in charge did not trust the order, partly because only one of their four missiles was targeted on Russia, and he saw no logic why missiles would be launched against China too, and because readiness was at DEFCON 2, not DEFCON 1.

9 Nov 1965, Nuke Detector Incident

The Command Center of the Office of Emergency Planning went on full alert after a massive power outage in the northeastern United States. Several nuclear bomb detectors—used to distinguish between regular power outages and power outages caused by a nuclear blast—near major US cities malfunctioned due to circuit errors, creating the illusion of a nuclear attack.

23 May 1967, Solar Flare Incident

A powerful solar flare accompanied by a coronal mass ejection interfered with multiple NORAD radars over the Northern Hemisphere. This interference was initially interpreted as intentional jamming of the radars by the Soviets, thus an act of war. A nuclear bomber counter-strike was nearly launched by the United States.

6 – 25 Oct 1973, Yom Kippur War – Israeli Nukes

During the Yom Kippur War, Israeli officials panicked that the Arab invasion force would overrun Israel after the Syrian Army nearly achieved a breakout in the Golan Heights, and the US government rebuffed Israel's request for an emergency airlift. According to a former CIA official, General Moshe Dayan requested and received authorization from Israeli Prime Minister Golda Meir to arm 13 Jericho missiles and 8 F-4 Phantom II fighter jets with nuclear warheads. The missile launchers were located at Sdot Micha Airbase, while the fighter jets were placed on 24-hour notice at Tel Nof Airbase. The missiles were said to be aimed at the Arab military headquarters in Cairo and Damascus. The crisis finally ended

when Prime Minister Meir halted all military action. Declassified Israeli documents have not confirmed these allegations directly, but have confirmed that Israel was willing to use "drastic means" to win the war.

6 – 25 Oct 1973, Yom Kippur War – Kincheloe Alarm Incident

The United States discovered Israel's nuclear deployment after a Lockheed SR-71 Blackbird reconnaissance aircraft spotted the missiles, and it began an airlift the same day. After the U.N. Security Council imposed a ceasefire, conflict resumed when the Israel Defense Force moved to encircle the Egyptian Third Army. According to former US State Department officials, General Secretary Leonid Brezhnev threatened to deploy the Soviet Airborne Forces against Israeli forces, and the US Armed Forces were placed at DEFCON 3. Israel also redeployed its nuclear weapons. While DEFCON 3 was still in effect, mechanics repairing the alarm system at Kincheloe Air Force Base in Michigan accidentally activated it and nearly scrambled the B-52 bombers at the base before the duty officer declared a false alarm.

9 Nov 1979 – NORAD Switched Tapes

Computer errors at the NORAD headquarters in Peterson Air Force Base, the Strategic Air Command command post in Offutt Air Force Base, the National Military Command Center in the Pentagon, and the Alternate National Military Command Center in the Raven Rock Mountain Complex led to alarm and full preparation for a nonexistent large-scale Soviet attack. NORAD notified national security adviser Zbigniew Brzezinski that the Soviet Union had launched 250 ballistic missiles with a trajectory for the United States, stating that a decision to retaliate would need to be made by the president within 3 to 7 minutes. NORAD computers then placed the number of incoming missiles at 2,200. Strategic Air Command was notified, and nuclear bombers prepared for takeoff. Within six to seven minutes of the initial response, PAVE PAWS satellite and radar systems were able to confirm that the attack was a false alarm. Congress quickly learned of the incident because Senator Charles H. Percy was present at the NORAD headquarters during the panic. A General Accounting Office investigation found that a training scenario was inadvertently loaded into an operational computer in the Cheyenne Mountain Complex. Commenting on the incident, US State Department adviser Marshall Shulman stated that "false alerts of this kind are not a rare occurrence. There is a complacency about handling them that disturbs me." Soviet General Secretary Leonid Brezhnev composed a letter to U.S. President Jimmy Carter that the false alarm was "fraught with a tremendous danger" and "I think you will agree with me that there should be no errors in such matters." In the months following the incident there were three more false alarms at NORAD, two of them caused by faulty computer chips. One of them forced the National Emergency Airborne Command Post to taxi into position at Andrews Air Force Base.

15 Mar 1980, False Missile Alert

A Soviet submarine near the Kuril Islands launched four missiles as part of a training exercise. Of these four, American early warning sensors suggested one to be aimed towards the United States. In response, the United States convened officials for a threat assessment conference, at which point it was determined to not be a threat and the situation was resolved.

26 Sep 1983, False Moscow Alert

Several weeks after the downing of Korean Air Lines Flight 007 over Soviet airspace, a satellite early-warning system near Moscow reported the launch of one American Minuteman ICBM. Soon after, it reported that five missiles had been launched. Convinced that a real American offensive would involve many more missiles, Lieutenant Colonel Stanislav Petrov of the Air Defense Forces refused to acknowledge the threat as legitimate and continued to convince his superiors that it was a false alarm until this could be confirmed by ground radar.

7 – 11 Nov 1983, Exercise Able Archer

Able Archer 83 was a command post exercise carried out by NATO military forces and political leaders between 7 and 11 November 1983.[37] The exercise simulated a Soviet conventional attack on European NATO forces 3 days before the start of the exercise (D-3), transitioning to a large scale chemical war (D-1) and on day 1 (D+1) of the exercise, NATO forces sought political guidance on the use of nuclear weapons to stem the Soviet advance which was approved by political leaders. NATO then began simulating preparations for a transition to nuclear war. These simulations included 170 radio-silent flights to air lift 19,000 US troops to Europe, regularly shifting military commands to avoid nuclear attack, the use of new nuclear weapon release procedures, the use of nuclear Command, Control, and Communications (C3) networks for passing nuclear orders, the moving of NATO forces in Europe through each of the alert phases from DEFCON 5 to DEFCON 1, and the participation of political leaders like Margaret Thatcher, Helmut Kohl and Ronald Reagan. The issue was worsened by leaders referring to B-52 sorties as "nuclear strikes", by the increased use of encrypted diplomatic channels between the US and UK,[40] and by the nuclear attack false alarm in September. In response, Soviet nuclear capable aircraft were fueled and armed ready to launch on the runway, and ICBMs were brought up to alert. Soviet leaders believed the exercise was a ruse to cover NATO preparations for a nuclear first strike and frantically sent a telegram to its residencies seeking information on NATO preparations for an attack. The exercise closely aligned with Soviet timeline estimations that a NATO first strike would take 7 to 10 days to execute from the political decision being made. Soviet forces stood down after 11 November when the exercise ended and NATO was not aware of the complete Soviet response until British intelligence asset Oleg Gordievsky passed on the information.

Aug 1990 – Feb 1991, Gulf War

During the Persian Gulf War, Ba'athist Iraq launched Scud missiles at Saudi Arabia and Israel and possessed a large cache of weapons of mass destruction. This, along with Saddam Hussein's previous threat to "burn half of Israel" with chemical weapons, led to fears that Saddam Hussein would order the use of the chemical weapons against the US-led coalition or against Israel. Israeli Prime Minister Yitzhak Shamir and Israeli Air Force Commander-in-Chief Avihu Ben-Nun both warned that an Iraqi chemical attack would trigger "massive retaliation", implying that Israel would retaliate with nuclear weapons. At the same time US Secretary of Defense Dick Cheney, General Norman Schwarzkopf Jr., and British Prime Minister Margaret Thatcher all emphasized that the use of WMD against Coalition forces would lead to a nuclear attack on Iraq. U.S. Secretary of State James Baker directly warned his counterpart Tariq Aziz that the United States had "the means to exact vengeance" in the event of an Iraqi resort to WMD. After the war, the Defense Intelligence Agency credited these threats with deterring Iraq from launching chemical attacks on Coalition forces. Nevertheless, Saddam Hussein did have a contingency plan to launch WMD-armed warheads at Tel Aviv in the event that he became cut off from the Iraqi Armed

Forces leadership or if the Iraqi government was about to collapse, which almost certainly would have triggered a retaliatory nuclear response from Israel. Saddam ultimately never deemed this option necessary because he never felt as if his government was about to collapse.

25 Jan 1995, Russian High Alert

Russian President Boris Yeltsin became the first world leader to activate the Russian nuclear briefcase after Russian radar systems detected the launch of what was later determined to be a Norwegian Black Brant XII research rocket being used to study the Northern Lights. Russian ballistic missile submarines were put on alert in preparation for a possible retaliatory strike. When it became clear the rocket did not pose a threat to Russia and was not part of a larger attack, the alarm was cancelled. Russia was in fact one of a number of countries earlier informed of the launch; however, the information had not reached the Russian radar operators. [39]

Post-Cold War

Although the Cold War never deteriorated into World War III, the US and Soviet Union did clash in proxy engagements during the Berlin Airlift (1948 – 1949), Korean War (1950 – 1953), Cuban Missile Crisis (1962), Vietnam War (1955 – 1975), and numerous lesser confrontations. Nearly a decade after the end of the Cold War the world was a different place. But instead of enjoying a peace dividend, the US military found itself more engaged than ever around the world.

Aug 1990 – Feb 1991, Gulf War

The Gulf War was an armed campaign waged by a 35-country military coalition in response to the Iraqi invasion of Kuwait. Spearheaded by the United States, the coalition's efforts against Iraq were carried out in two key phases: Operation Desert Shield, which marked the military buildup from August 1990 to January 1991; and Operation Desert Storm, which began with the aerial bombing campaign against Iraq on January 17, 1991 and came to a close with the American-led Liberation of Kuwait on February 28, 1991. [40]

Mar 1991 – Dec 1996, Operation Provide Comfort

Operation Provide Comfort and Provide Comfort II were military operations initiated by the United States and other Coalition nations of the Persian Gulf War, starting in April 1991, to defend Kurdish refugees fleeing their homes in northern Iraq in the aftermath of the Gulf War, and to deliver humanitarian aid to them. The no-fly zone instituted to help bring this about would become one of the main factors allowing the development of the autonomous Kurdistan Region. [41]

Mar 1991 – Dec 1996, Iraqi No-Fly Zones

The US, United Kingdom, and its Gulf War allies declared and enforced "no-fly zones" over the majority of sovereign Iraqi airspace, prohibiting Iraqi flights in zones in southern Iraq and northern Iraq, conducting aerial reconnaissance, and several specific attacks on Iraqi air-defense systems as part of the UN mandate. Often, Iraqi forces continued throughout the decade by firing on US and British aircraft patrolling no-fly zones. [42]

Jul 1992 – Jan 1996, Operation Provide Promise

Operation Provide Promise was a humanitarian relief operation in Bosnia and Herzegovina during the Yugoslav Wars, from July 2, 1992 to January 9, 1996. By the end of the operation, aircraft from 21 countries had flown 12,886 sorties into Sarajevo, delivering 159,622 tons of food, medicine, and supplies and evacuating over 1,300 wounded people. The US flew 3,951 C-130, 236 C-141, and 10 C-17 airland sorties (delivering 62,801.5 tons), as well as 2,222 C-130 air-drop sorties. Provide Promise was one of the longest running humanitarian airlifts in history. [43]

Apr 1993 – Dec 1995, Operation Deny Flight

On April 12, 1993, in response to a United Nations Security Council passage of Resolution 816, U.S. and NATO enforced the no-fly zone over the Bosnian airspace, prohibited all unauthorized flights and allowed to "take all necessary measures to ensure compliance with [the no-fly zone restrictions]." [44]

3 – 4 Oct 1993, Battle of Mogadishu (Blackhawk Down Incident)

Task Force Ranger, made up largely of the 75th Ranger Regiment and Delta Force entered hostile urban area Mogadishu to seize two high ranking Somali National Army leaders. Two American UH-60 Black Hawks are shot down, 18 Americans are killed in action, with another 73 wounded, and 1 captured. The events of the battle were gathered in the book Black Hawk Down, which was later adapted to a movie of the same name. [45]

July 1994 – March 1995, Operation Uphold Democracy

In 1994 US Navy ships began an embargo against Haiti. Up to 20,000 US military troops were later deployed to Haiti to restore democratically elected Haiti President Jean-Bertrand Aristide from a military regime which came into power in 1991 after a major coup. [46]

Aug – Dec 1995, Operation Deliberate Force

On August 30, 1995, US and NATO aircraft began a major bombing campaign of Bosnian Serb Army in response to a Bosnian Serb mortar attack on a Sarajevo market that killed 37 people on August 28, 1995. This operation lasted until September 20, 1995. The air campaign along with a combined allied ground force of Muslim and Croatian Army against Serb positions led to a Dayton Agreement in December 1995 with the signing of warring factions of the war. As part of Operation Joint Endeavor, U.S. and NATO dispatched the Implementation Force (IFOR) peacekeepers to Bosnia to uphold the Dayton agreement. [47]

Dec 1995 – Dec 1996, Operation Joint Endeavor

Beginning in December 1995, US and allied nations deployed peacekeeping forces to Bosnia in support of Operation Joint Endeavor. Task Force Eagle, comprised of 20,000 American soldiers, was the US component of NATO's Implementation Force (IFOR) and was tasked with implementing the military elements of the Dayton Peace Accords in support of Operation Joint Endeavor. Task Force Eagle was the lead element for NATO's Multinational Division (North) or MND(N). Operation Joint Endeavor marked the first commitment of forces in NATO's history, as well as the first time since World War II that American and Russian soldiers had shared a common mission. Thousands of people were alive in Bosnia because of these soldiers' service. On 20 December 1996, the IFOR mandate ended and NATO

established a new operation, Operation Joint Guard, along with a new Stabilisation Force (SFOR) to replace IFOR. Task Force Eagle remained the title for the US contingent supporting this new operation. [48]

24 Mar – 10 Jun 1999, Operation Allied Force

US and NATO aircraft began a major bombing of Serbia and Serb positions in Kosovo on March 24, 1999, during the Kosovo War due to the refusal by Serbian President Slobodan Milošević to end repression against ethnic Albanians in Kosovo. This operation ended on June 10, 1999, when Milošević agreed to pull his troops out of Kosovo. In response to the situation in Kosovo, NATO dispatched the KFOR peacekeepers to secure the peace under UNSC Resolution 1244. [49]

9/11

On the morning of September 11, 2001, 19 hijackers formed into four teams and made their way to three airports. Within a matter of hours they successfully negotiated security measures designed to flag suspicious passengers and screen for weapons. At 7:59 am, the first team took off from Boston Logan airport aboard a Boeing 757 fueled for transcontinental flight. Within 40 minutes, all four teams were airborne aboard similar flights originating from Logan, Dulles, and Newark airports.

Shortly after gaining cruising altitude, the hijackers attacked. They subdued the cabin using pepper spray and razor knives before forcing their way into the cockpit and killing the pilot and copilot. Once in control, they disengaged the transponder and dove the aircraft to lower altitude, effectively disappearing from FAA tracking screens.

At 8:46 am, the first aircraft crashed into the North Tower of the World Trade Center. Loaded with fuel, the aircraft disintegrated into a giant fireball as it ploughed into the skyscraper. Within minutes, dramatic video was broadcast across network television news. Fifteen minutes later, a second aircraft crashed into the South Tower. The United States was under attack.

Fighter interceptors were scrambled from Langley Air Force Base in Virginia. But in the confusion of events, they were directed out over the Atlantic to intercept expected enemy military aircraft. A little over 30 minutes after the second crash, a third aircraft crashed into the Pentagon. The alert fighters were too far away to do anything.

Passengers aboard the fourth aircraft were warned about the suicide hijackings by cell phone. As the aircraft flew towards Washington DC, passengers and crew rose up against the hijackers. Flight recorders captured the sound of passengers trying to force their way into the cockpit when the hijackers decided to dive the aircraft into the ground. At 10:03, the last hijacked aircraft crashed into the countryside outside Shanksville Pennsylvania.

From start to end, the attacks had taken a little over two hours. More than 2,600 people died at the World Trade Center, including 333 firefighters; 125 died at the Pentagon; and 256 passengers died aboard the four aircraft. All told, the attacks resulted in 3,000 deaths and $40 billion in damages.

The death toll was greater than that at Pearl Harbor on December 7, 1941. But where the destruction at Pearl Harbor was inflicted by an armada of the Imperial Japanese Navy, the destruction on 9/11 was caused by only 19 young men, most from Saudi Arabia. Some had been in the United States for more than a year. Though four had pilot training, most were not well-educated. Most spoke English poorly, and some hardly at all.

The ensuing investigation by the 9/11 Commission estimated the cost of the attack at less than $400,000. It's most distinguishing feature, they said, was its "surpassing disproportion". The hijackers

had turned passenger jets into guided missiles. Instead of using WMD, they had achieved WMD effects by subverting the aviation infrastructure. [1]

USNORTHCOM

On September 11, 2001, President Bush was seated in a Florida classroom when at 9:05 am his Deputy Chief of Staff whispered "A second plane hit the second tower. America is under attack." President Bush was quickly taken to Air Force One and flown to Offutt Air Force Base in Omaha Nebraska, headquarters for United States Strategic Command (USSTRATCOM). The four-star Commander of USSTRATCOM had direction and control over the US nuclear triad. It quickly became apparent that the attacks against the World Trade Center in New York and the Pentagon in Virginia were not the opening salvos of a nuclear war. This was a conventional attack, the first since the Japanese attacked Pearl Harbor almost sixty years earlier. Given the creation and evolution of the Unified Command Plan since World War II, the President of the United States as Commander in Chief of the armed forces was now faced with the prospect of coordinating the nation's conventional defenses across four separate unified commands: Joint Forces Command to protect the East Coast, Pacific Command to secure the West Coast, Southern Command to secure the Gulf approaches, and NORAD to protect the skies over North America. The arrangement proved unwieldy. [50]

Examination of the flight manifests identified the hijackers as members of al Qaeda, a designated terrorist organization headed by Osama Bin Laden, a Saudi exile now living and directing terrorist operations from Afghanistan under the protection of the Taliban government. The National Security Council spent the next ten days after 9/11 preparing diplomatic and military options together with US Central Command in who's AOR Afghanistan was situated. On September 22, 2001 in a speech before Congress, President Bush sent an ultimatum to the Taliban: Give up al Qaeda or share their fate. "Either you are with us, or you are with the terrorists." The Taliban refused to give up Bin Laden. On October 7, USCENTCOM launched Operation ENDURING FREEDOM to remove the Taliban, eliminate al Qaeda, and capture or kill Osama bin Laden. With the aid of US airpower, the Northern Alliance was able to overcome their Taliban enemy and defeat them in battle. By March 2022, al Qaeda was in shambles, the Taliban were in flight, and Bin Laden was in hiding. By April 2022, the US military and its allies took up an occupying position in Afghanistan to help stabilize the new government, keep a lid on al Qaeda and the Taliban, and find Osama Bin Laden. [1]

After things began to settle in Afghanistan, President Bush started addressing some of the security problems exposed on 9/11, not least of which was the defense of the continental United States. In April 2002 President Bush approved a revision to the Unified Command Plan creating US Northern Command. USNORTHCOM activated October 1, 2002 and became fully operational a year later. After the debacle on 9/11, USNORTHCOM was given responsibility for the air, land, and maritime defense of the entire continental United States. The President no longer had to deal with four commands, only one. [50]

United States Northern Command is one of six Geographic Combatant Commands (GCCs) within the Department of Defense (DOD) operational chain of command authorized to plan and execute US military missions within its designated Area of Responsibility (AOR). The USNORTHCOM AOR encompasses all of North America including Canada and Mexico and the surrounding water out to 500 nautical miles, plus the Bahamas, Puerto Rico, and US Virgin Islands. USNORTHCOM headquarters are located on Peterson Air Force Base in Colorado Springs, Colorado. The four-star Combatant Commander (CCDR) is charged with accomplishing tasks assigned by the President or Secretary of Defense. The CCDR

USNORTHCOM is charged with engaging in multinational security cooperation, particularly defense of US and Canadian airspace through the auspices of the North American Aerospace Defense Command (NORAD), providing Defense Support of Civil Authorities (DSCA) to State, Local, Tribal, and Territorial (SLTT) governments when requested and approved, and conducting Homeland Defense (HD). [51]

USNORTHCOM maintains 24-hour watch over its AOR from its headquarters on Peterson Air Force Base. USNORTHCOM also maintains close contact with other military command posts and US Government watch centers, and agencies representing Canada and Mexico. Although USNORTHCOM has no permanently assigned forces, it does stand ready to direct military actions in the land, air, maritime, and space domains through the auspices of its assigned military components.

Land Component

United States Army North (ARNORTH) based out of Fort Sam Houston in San Antonio Texas is the Joint Force Land Component Commander (JFLCC) for USNORTHCOM. In the very unlikely event the US faced full-scale land invasion by a hostile power, USNORTHCOM would prevail on ARNORTH to advise and direct assigned ground forces to defeat the enemy. Ground forces assigned to ARNORTH may be comprised of both US Army and US Marine units. ARNORTH may also request the National Guard. Although ARNORTH is ready and capable to command combat operations, it is more likely in today's security environment to conduct force protection (FP) and critical infrastructure protection (CIP) missions when directed by the President or Secretary of Defense. Force Protection missions would strengthen defenses at military installations, and CIP would extend physical protection to vital infrastructure facilities. [52]

Air Component

NORAD has responsibility for aerospace control including air sovereignty and air defense of US and Canadian airspace. By treaty, the Commander USNORTHCOM also holds the position as Commander or Deputy Commander of NORAD. NORAD headquarters and watch center are co-located with USNORTHCOM on Peterson Air Force Base. NORAD routinely maintains forces on alert for homeland air defense, cruise missile defense, and aerospace control alert missions against long-range incursions. For flexibility and survivability reasons, NORAD is divided into three major sectors: 1) ANR, 2) CANR, and 3) CONR. ANR based out of Joint Base Elmendorf in Anchorage maintains watch over Alaska. CANR based out of Canadian Forces Base (CFB) Winnipeg in Manitoba maintains watch over Canada. And CONR based out of Tyndall Air Force Base Florida maintains watch over the Continental United States (CONUS).[5] The CONR commander is also the United States Air Forces North (AFNORTH) commander and may be designated the Joint Force Air Component Commander (JFACC) for unilateral US air operations within the USNORTHCOM AOR. [52]

Maritime Component

United States Fleet Forces Command (USFF) headquartered at Naval Support Activity Hampton Roads in Norfolk Virginia is the designated Commander of United States Naval Forces for Northern

[5] CONR is further divided into three subsectors: 1) EADS based out of Rome Air National Guard Base New York maintains watch over the eastern US, 2) WADS based out of Joint Base Lewis-McChord in Washington maintains watch over the western US, and 3) NCR-IADS which manages Integrated Air Defenses (IADs) over the National Capital Region (NCR) surrounding Washington DC.

Command (COMUSNAVNORTH) and may also be designated the Joint Force Maritime Component Commander (JFMCC) for military operations in US territorial waters. Fleet Forces Command will assign operational control of US Navy forces when directed by the President or Secretary of Defense. The US Second Fleet co-located with USFF headquarters in Norfolk Virginia operates in the North Atlantic off the East Coast. The US Third Fleet headquartered at Naval Base Point Loma in San Diego California operates in the Eastern Pacific off the West Coast. Although the threat of maritime invasion is unlikely, when directed by the President, maritime forces may be employed to conduct combat operations and active and passive defense-in-depth to counter maritime attacks within US territorial waters. [52]

Space Component

Ballistic Missile Defense (BMD) is an essential component of USNORTHCOM's space domain responsibilities. USNORTHCOM has operational control of the 100th Missile Defense Brigade which operates the Ground-based Midcourse Defense (GMD) anti-ballistic missile system. GMD is comprised of 44 Ground Based Interceptors (GBIs) located at Vandenberg Air Force Base California and Fort Greely Alaska. The GBI carries an inert payload that destroys an incoming warhead by direct impact during the midcourse phase of the ICBM flight outside the Earth's atmosphere. The 100th Missile Defense Brigade stationed at Schriever Air Force Base Colorado is a component of US Army Space and Missile Defense Command. [52]

Cyber Defense

US Cyber Command can support cyberspace operations (CO) within the USNORTHCOM AOR and assist with expertise and capabilities when authorized. Co-located with the National Security Agency (NSA) headquarters on Fort George G. Meade in Maryland, USCYBERCOM became an independent unified combatant command in August 2017. USCYBERCOM conducts both Defensive Cyber Operations (DCO) and Offensive Cyber Operations (OCO). Cyber operations are performed by 6,200 military and civilian personnel organized into 133 teams comprising the Cyber Mission Force (CMF):

1. **Cyber Protection Teams** act to defend the Department of Defense Information Network (DODIN), critical infrastructure, and key resources while also working to prepare other cyber forces for combat. There are 68 Cyber Protection Teams.

2. **Cyber Combat Mission Teams** conduct military cyber operations in support of combatant commands. There are 27 Cyber Combat Mission Teams.

3. **Combat Support Teams** provide support to National Mission and Combat Mission teams. There are 25 Cyber Support Teams.

4. **Cyber National Mission Teams** defend the Nation by observing adversary activity, defending against attacks, and maneuvering to defeat them. There are 13 National Mission Teams. [53]

Nuclear Deterrence

Headquartered at Offutt Air Force Base Nebraska, United States Strategic Command is responsible for strategic nuclear deterrence and global strike. It also provides integrated missile defense

and global command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). The USSTRATCOM Global Operations Center (GOC) maintains situational awareness for the commander and is the mechanism by which he exercises operational command and control of the US strategic triad. The Alternate Processing and Correlation Center in the USSTRATCOM Underground Command Complex at Offutt AFB provides an alternate missile warning correlation center to the Cheyenne Mountain Missile Warning Center. It is the prime source of missile warning data for USSTRATCOM. USSTRATCOM also maintains an Airborne Command Post (ABNCP) called "Looking Glass" providing the ability to command, control, and communicate with its nuclear forces should ground-based command centers become inoperable. [54]

Nuclear Command & Control

The US President has sole authority to authorize the use of US nuclear weapons. This authority is inherent in his constitutional role as Commander in Chief. The President can seek counsel from his military advisors; those advisors are then required to transmit and implement the orders authorizing nuclear use. The President, however, does not need the concurrence of either his military advisors or the U.S. Congress to order the launch of nuclear weapons. Neither the military nor Congress can overrule these orders.

The Nuclear Command and Control System (NCCS) provides the President with the means to authorize the use of nuclear weapons in a crisis and to prevent unauthorized or accidental use. The NCCS collects information on threats to the United States, communicates that information to the President, advises the President on response options, communicates the President's chosen response to the forces in the field, and controls the targeting and application of those forces. Within this system, radars, satellites, and processing systems provide unambiguous, reliable, accurate, and timely warning about attacks on the United States, its allies, and its forces overseas. If the NCCS identified an attack or an anomalous event, the President would participate in an emergency communications conference with the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and other military advisors. They would offer the President details and an assessment of the possible incoming attack, while the commander USSTRATCOM would explain the President's options for a retaliatory attack.

If notified of a potential nuclear attack, the President would evaluate and respond to this information and decide whether to authorize the use of US nuclear weapons. He would communicate his choices and provide this authorization through a communications device known as the nuclear "football"—a suitcase carried by a military aid who is always near the President. The suitcase is equipped with communication tools and a book with prepared war plans for certain targets. The President could choose from these prepared plans or, time permitting, ask USSTRATCOM to prepare an alternative.

If the President chooses to respond with a nuclear attack, he would identify himself to military officials at the Pentagon with codes unique to him. These codes are recorded on an ID card, known as the "biscuit," that the President carries at all times. Once identified, he would transmit the launch order to the Pentagon and USSTRATCOM. The Secretary of Defense would possibly contribute to the process by confirming that the order came from the President, but this role could also be filled by an officer in the National Military Command Center (NMCC) at the Pentagon.

Once the President makes his decision, USSTRATCOM prepares the weapons needed for the selected option. When the order is transmitted it is immediately executed. Minuteman missiles can fire

in two minutes. Submarine launched missiles can fire in 15 minutes. There is no way to reverse a launch order once given. There is no way to recall or destroy missiles once they're launched.

Built during the Cold War, the NCCS was designed for speed and decisiveness, not debate and decision. This is because ICBMs launched from Russia could reach the US in 30 minutes; sea-based missiles launched off the US coast might arrive in 15 minutes. If the United States wanted to retaliate before US weapons, or, more importantly, the US command and control system were degraded by an attack, then the entire process of identifying, assessing, communicating, deciding, and launching would have to take place in less than that amount of time. Given that some time would be needed for mechanical or administrative steps, analysts estimate that the President would have less than 10 minutes to absorb the information, review his options, and make his decision. [55]

Nuclear Response Options

During the Cold War, US doctrine argued that, to deter a Soviet attack, the United States would need to be able to retaliate even if the Soviet Union launched a massive attack with little warning. Hence, the United States planned for scenarios where the Soviet Union launched thousands of nuclear warheads that could reach the United States. The short timelines and preplanned responses left the President with little option but to launch US weapons before most of the attacking warheads detonated on US soil.

But, even during the Cold War, an attack or anomalous event was not the only possible scenario for the start of a nuclear war, and a massive US response was not the only option available to the President. If a nuclear war escalated out of a conflict in Europe, or if the Soviet Union launched a more measured attack, the President might have more time to assess the threat and consider an appropriate response. Moreover, because US bombers could fly away from their bases earlier in a crisis or conflict and US ballistic missile submarines might survive an attack on US territory, the President didn't necessarily have to launch immediately upon warning. Nevertheless, some analysts have speculated that a launch under attack was the dominant option during the Cold War, and that the nuclear command and control system was designed to facilitate the prompt launch of US nuclear weapons.

The United States has reviewed and revised its nuclear employment plans several times since the end of the Cold War. According to unclassified reports, these reviews have added options to the plans available to the President. While some options probably still provide responses to an attack from a nation, like Russia, with a large nuclear force, others might provide for more measured and discriminate attacks. In addition, even though the plans likely include options for a prompt response in the face of an unexpected attack, they also likely have options for delayed responses. As a result, although the prompt launch options may have dominated US planning during the Cold War, they may no longer dominate US nuclear war plans.

Another scenario could see the United States choose to use nuclear weapons prior to a nuclear attack against the United States or its allies, on a timeline that did not reflect an imminent nuclear attack against the United States. The United States has never declared a "no first use" policy, and the President could order the first use of nuclear weapons. As noted above, his military advisors may seek to adjust his orders to meet the laws of armed conflict, but there is, otherwise, no legal barrier to first use.

Some analysts outside the US government have questioned whether the United States should retain the option to launch nuclear weapons promptly because, they argue, the time pressures could lead to the accidental or inadvertent start of a nuclear war. They note that the United States received false warning of nuclear attack several times during the Cold War, and if the President had responded

within 30 minutes it would have triggered global nuclear war. If the President could not launch the weapons in such haste, he would necessarily have the time to wait for more accurate or less ambiguous information.

Others, however, argue that there is nothing inherently destabilizing or dangerous in the prompt launch options. The President has options to delay a response and await additional information. In addition, even in the current security environment, a President and his advisors would be unlikely to interpret ambiguous warning information as evidence of an all-out attack from Russia or another nation. Instead, they note that the presence of both prompt and delayed options bolsters deterrence by providing the President with the flexibility to choose the appropriate response to an attack on the United States or its allies. [55]

2022 National Defense Strategy

The 2022 National Defense Strategy (NDS) of the United States is deterrence. The DOD will develop and maintain capabilities and conduct military operations to deter attack against the United States and its Allies.

According to the 2022 NDS, deterrence is strengthened by actions that reduce a competitor's perception of the benefits of aggression relative to restraint. Effective deterrence requires the DOD to consider how competitors perceive the US and its Allies' commitment and combat credibility; their perception of their own ability to control escalation risks; and their view about the consequences of their actions. Actions aimed at strengthening deterrence work by different logics: denial, resilience, and cost imposition.

Deterrence by Denial. To deter aggression, especially where potential adversaries could act to seize territory, the DOD will develop asymmetric approaches and optimize our posture for denial. In the near-term, we will continue to develop innovative operational concepts and supplement current capabilities and posture through investments in mature, high-value assets. Over the mid- to long-term, we will develop new capabilities including long-range strike, undersea, hypersonic, and autonomous systems, and improve information sharing and the integration of non-kinetic tools.

Deterrence by Resilience. Denying the benefits of aggression also requires resilience – the ability to withstand, fight through, and recover quickly from disruption. The DOD will improve its ability to operate in the face of multi-domain attacks on a growing surface of vital networks and critical infrastructure, both in the homeland and in collaboration with Allies and partners at risk. Because the cyber and space domains empower the entire Joint Force, we will prioritized building resilience in these areas. Cyber resilience will be enhanced by, for example, modern encryption and a zero-trust architecture. In the space domain, the DOD will reduce adversary incentives for early attack by fielding divers, resilient, and redundant satellite constellations. We will bolster our ability to fight through disruption by improving defensive capabilities and increasing options for reconstitution. We will assist Allies in doing the same.

Deterrence by Cost Imposition. Denial and resilience strategies are necessary but not always sufficient. Effective deterrence may also hinge on our ability to impose costs in excess to the perceived benefits of aggression. The DOD will continue to modernize our nuclear forces, the ultimate backstop to deter attacks on the homeland and our Allies and partners who rely on US extended deterrence. Direct cost imposition approaches also include a broad range of other means, including conventional long-range fires, offensive cyber, irregular warfare, support for foreign internal defense, and interagency instruments, such as economic sanctions, export controls, and diplomatic measures. [56]

2022 Homeland Defense Strategy

The 2022 National Defense Strategy of the United States promulgates a strategy to deter attacks against the US Homeland. According to this strategy, the DOD will take steps to raise potential attackers' direct and indirect costs while reducing their expected benefits for aggressive action against the homeland, particularly by increasing resilience. The DOD will ensure that hostile operations – including those conducted early in a crisis or conflict – will not advance adversary objectives or severely limit US response options. The DOD will work to prioritize closer coordination with US interagency, state, local, tribal, and territorial partners, as well as with the private sector, starting with the defense industrial base.

"From Stettin in the Baltic to Trieste in the Adriatic an iron curtain has descended across the Continent."
- Winston Churchill, address at Westminster College, Fulton, Missouri, March 5, 1946

Part 3: Civil Defense

Civil Defense has no formally agreed definition, but it is generally accepted to mean the protection of domestic civilian populations from deliberate attack. The 1950 Civil Defense Act was established to protect the US population from Soviet nuclear attack during the Cold War. The Cold War ended when the Soviet Union collapsed in December 1991. The Civil Defense Act was repealed in 1994, and its remaining authorities amended to Title VI of the 1988 Stafford Act. These were assumed by the Federal Emergency Management Agency (FEMA) that was formed in 1979 by Executive Order 12148 and then incorporated into the new Department of Homeland Security when it was created by the 2002 Homeland Security Act.

In 2017, Quin Lucie, a FEMA attorney and former Marine Corps judge advocate conducted a thorough analysis of the agency's role in Civil Defense (CD). He found that 1) the agency retains statutory CD responsibilities based on the original 1950 Civil Defense Act under Title 50 Section 3042 of United States Code (USC); 2) that with the end of the Cold War and ascension of Director James Witt in 1993, the agency's primary focus became Emergency Preparedness (EP) for natural disasters at the expense of CD which has been reduced and marginalized to the point that it on longer remains in the FEMA lexicon; and 3) in light of increasing confrontation with Russia, China, and North Korea, and new means at their disposal for directly attacking the US, FEMA must revive and re-invest in CD to ensure the US can quickly respond and recover from these emerging new threats to its territory and population. Based on his findings, Mr. Lucie proposed reviving and re-invigorating a Civil Defense program oriented towards three main objectives: 1) Protecting the population, defense industrial base, key critical infrastructure, and the functions of government; 2) Supporting Department of Defense (DoD) efforts to deploy military capabilities while under attack; and 3) Mobilizing and sustaining the nation's manpower and defense industrial base during a time of war. [57]

Written as it was in 2017, five years before the present crises emerged in the Ukraine, we will go back and take a closer look at events Mr. Lucie cites in supporting his arguments as well as those that have occurred since he submitted his paper for publication. Furthermore, we will examine his proposals and use them to guide a comparison between Cold War Civil Defense programs and contemporary Emergency Preparedness programs. From this comparison we will develop new findings and use them to support independent recommendations for addressing Homeland Defense and Civil Defense in the 21st Century.

Civil Defense Evolution

What is Civil Defense? According to Mr. Lucie, the term "civil defense" has been replaced in FEMA by "emergency preparedness" and the last surviving official use of the term may be found in Section 312.2, Title 44 of the Code of Federal Regulations (CFR), which states:

> *"The term civil defense means all those activities and measures designed or undertaken (1) to minimize the effects upon the civilian population caused, or which would be caused by an attack upon the United States, or by natural disaster, (2) deal with the immediate emergency conditions which would be created by any such attack, or natural disaster, and (3) to effectuate emergency repairs to, or the emergency restoration of vital utilities and facilities destroyed or damaged by any such attack or natural disaster…"*

World War to Cold War

Civil Defense arose in England during World War I out of concerns for protecting its domestic territory and population from direct enemy attack by air. In 1915, Germany conducted seven air strikes against London. Civil Defense became a concern to all combatants during World War II as each side waged aerial bombardment campaigns against the territory and population of the other. Although the US remained mostly immune from direct attack during World War II,[6] it created the Office of Civilian Defense (OCD) in May 1941. The OCD supervised and coordinated the efforts of an estimated 11 million volunteers to provide air raid warning and sheltering, emergency firefighting support, and other designated "war services". The OCD was terminated by Executive Order 9562 in June 1945 one month after Germany's surrender.

After the war, relations between the US and its former ally the Soviet Union quickly deteriorated as Stalin sought to impress communism upon those territories his forces occupied. The Cold War began March 12, 1947 when the American policy of Soviet containment was formalized in the Truman Doctrine. Although the doctrine sought to avoid direct military confrontation, the US monopoly in atomic weapons gave it a strategic advantage against the numerically superior Soviet conventional forces. It was this US atomic advantage that perhaps prevented the numerically superior Soviet Union from overrunning the allies and instead implementing a blockade that precipitated the 1948-49 Berlin Airlift. The US advantage ended when the Soviet Union successfully tested its own atomic bomb in August 1949. With it came the prospect of direct Soviet attack on the US should the Cold War turn hot. State and Local officials began to demand from the Federal government a clear outline of what they were to do when crisis situations arose. Congress responded by passing the Federal Civil Defense Act of 1950. Signed by President Truman, the law created the Federal Civil Defense Administration (FCDA) to formulate national policy and guide the States in helping protect their citizens.

The 1950 Federal Civil Defense Act allocated significant funding to build bomb shelters. The law allowed the FCDA to develop shelter designs and make financial contributions to shelter programs. However, Congress stipulated that the Federal government could not finance the construction of new bomb shelters. In communities across the country there was great debate over the necessity of bomb shelters in case of nuclear attack. Grim predictions concerning the aftermath of a nuclear attack swayed the arguments in a manner that generally discouraged public interest in building bomb shelters. In 1953 the Soviets detonated a hydrogen bomb. The blast and thermal effects of this new fusion weapon were so destructive that many experts argued that bomb shelters would be useless. As a result, the new FCDA Administrator urged Congress to scale back or completely eliminate funding for shelter programs. Interested in balancing the budget, President Eisenhower endorsed evacuations over sheltering. The idea was to disperse city populations to the countryside upon warning of attack. That idea lost its appeal after fallout from the 1954 Bravo test shot unintentionally spread radiation over 7,000 square miles of the Pacific. The 23 crew members of a Japanese fishing vessel were all poisoned as were the 64 inhabitants of Rongelap Atoll. All suffered vomiting, diarrhea, and skin burns from acute radiation sickness. Rongelap was evacuated and not declared safe until 2014. The incident resurrected the

[6] Japan attacked US territories in Hawaii and the Marshall Islands, and successfully occupied US territories in Guam, Philippines, and Alaska. In February 1942 a Japanese submarine fired twenty-five shells from its deck gun at the Bankline oil refinery west of Santa Barbara California. Little damage and no casualties were reported. Starting in November 1944, Japan launched some 9,000 high-altitude balloons tethered with explosives targeting the US. Perhaps 1,000 reached North America, 285 were spotted in the Pacific Northwest, and six picnickers killed in Oregon when a balloon bomb they dragged from the woods exploded.

concept of sheltering but to protect from fallout not blast effects. The new FCDA policy was "evacuation to shelter".

Less robust than bomb shelters, fallout shelters were also less expensive, but still they were not cheap. In 1956 the FCDA proposed a federally subsidized National Shelter Program at the cost of $32 billion. Although endorsed by studies, the proposal died from lack of political support. President Kennedy supported sheltering. He believed it was necessary in case deterrence failed against an irrational enemy. In November 1961, President Kennedy's top advisors determined that the primary role of the Federal government in Civil Defense was to provide community shelters. In September 1961 he commissioned a survey of available public fallout shelters. To qualify, the facility had to have enough space for at least 50 people, include one cubic foot of storage space per person, and have a radiation protection factor of 100. The DOD was tasked with furnishing supplies to local governments which were then responsible for stocking their shelters. By 1963, qualifying shelter space was identified for 104 million people, and enough supplies stocked for 9 million. This means at the height of the Cold War during the Cuban Missile Crisis, the US had sufficient shelter space to protect perhaps 57% of the population but sustain only 5% following a nuclear exchange with the Soviet Union.[7]

President Johnson's administration marked the beginning of a drastic cutback in funding for Civil Defense programs. Although the nation had invested in nuclear deterrence and missile defenses, Secretary of Defense McNamara believed a viable sheltering program was still necessary in case either of these failed. But as Civil Defense began to fall slowly off the public radar, President Johnson chose not to pursue it. By the time President Nixon entered office, public and government interest in Civil Defense had fallen precipitously from its peak in the early 1960s. By the same token, Hurricane Camille in August 1969 had made the public acutely aware of the Federal government's lack of preparedness for responding to natural disasters. President Nixon ordered a comprehensive review. National Security Study Memorandum 57 released in June 1970 concluded that the nation's preparedness for natural disasters was minimal to nonexistent. As a result, the Administration issued National Security Decision Memorandum (NSDM) 184 recommending a "dual-use" approach for Civil Defense. Federal funds allocated to prepare for military attack could now be shared with State and Local governments to prepare for natural disasters. The "dual-use" approach was built on the premise that the same preparations for evacuation, communications, and survival are common to both natural disasters and military attack. The "dual-use" approach was attractive to State and Local governments who had previously been reluctant to participate in nuclear attack planning. It also garnered support of the American public who viewed planning for natural disasters as more productive use of taxpayer money.

Attractive as it was, the "dual-use" approach to Civil Defense was suspended under President Ford after it was discovered that the Soviet Union was aggressively building public fallout shelters. It looked to some as if the Soviet Union thought it could avoid Mutual Assured Destruction (MAD) and possibly win a nuclear war with the US. Civil Defense again became a priority and the US needed to catch up but undertaking a massive shelter construction program remained too expensive. The adopted alternative was the Crisis Relocation Program (CRP). Under CRP, urban residents would be relocated to rural host counties. CRP evacuation planning was conducted by the States with Federal funds that also provided support for relocation, food distribution, and medical care. The program was criticized for its reliance on a relatively long warning time of 1 to 2 days which might or might not play out as it did during the 1962 Cuban Missile Crisis. Others doubted whether large-scale evacuation through

[7] US population in 1962 was 181,917,809.

bottlenecked transportation routes was even feasible. Despite the criticisms, CRP remained the focus of Civil Defense efforts under both President Ford and President Carter. As stated in a 1979 FEMA report, CRP was seen as a "low-cost survival alternative" and necessary counter to well-funded and extensive Soviet evacuation programs.

The biggest change to Civil Defense under President Carter was creation of the Federal Emergency Management Agency. The consolidation of Civil Defense under FEMA represented only the latest but not the last shuffling of Civil Defense responsibilities within the Federal Government. Civil Defense was first invested in the Federal Civil Defense Administration when the Federal Civil Defense Act was passed and signed by President Truman in 1950. In 1958 President Eisenhower consolidated the functions of the FCDA together with the Office of Defense Mobilization to create the Office of Civil and Defense Mobilization (OCDM) within the Executive Office of the President. The OCDM was short lived. In August 1961 OCDM was split by President Kennedy into the Office of Emergency Planning (OEP), tasked with advising and assisting the President on Civil Defense, and the Office of Civil Defense (OCD) tasked with overseeing Civil Defense programs from the Pentagon. In May 1972 President Nixon renamed OCD the Defense Civil Preparedness Agency (DCPA), and in June 1973 closed the OEP and distributed its functions among other executive agencies. Coordination problems stemming from this fragmentation of Civil Defense responsibilities started to become painfully apparent under the Ford Administration. Upon taking office President Carter commissioned a review of the disjointed system of bureaucracies managing Civil Defense. Presidential Review Memorandum 32 in September 1977 recommended consolidating Civil Defense functions into one coherent agency in direct contact with the White House. Then on March 28, 1979, the nuclear energy plant on Three Mile Island near Harrisburg PA suffered a partial meltdown. The ensuing Federal response was slow, poorly coordinated, and badly communicated. The accident dramatically demonstrated the need for more effective Federal emergency management. On July 20, 1979, President Carter issued Executive Order 12148 creating FEMA.

President Reagan was a vocal critic of the Soviet Union. During Reagan's Administration, tensions between the two countries mounted to levels not experienced since the Kennedy Administration. National Security Decision Directive 26 in February 1982 stated that "it is a matter of national priority that the United States have a Civil Defense program which provides for the survival of the U.S. population." This made nuclear preparedness a top priority for FEMA, and again emphasized CRP evacuation at the expense of dual-use technology. Congress, wary of the President's hawkish stance, amended the 1950 Civil Defense Act allowing all future funds to become dual-use, available for purposes of natural disasters and military attack. In 1983, FEMA responded to the Congressional push for more peacetime disaster preparation with plans for an Integrated Emergency Management System (IEMS) to develop all-hazard preparedness plans at the Federal and State levels. In the final years of his administration, President Reagan made concessions to Congress too. In November 1988 he signed into law amendments to the 1974 Disaster Relief Act, better known today as the Stafford Act. The Act defined the disaster declaration process and provided the statutory authority for Federal assistance during a disaster.

Under President George H. W. Bush, tensions between East and West rapidly began to de-escalate when the soviet empire started disintegrating after the fall of the Berlin Wall in November 1989. The Cold War ended when the Soviet Union was dissolved on December 26, 1991. The threat of nuclear attack on the US evaporated almost overnight. As a result, Civil Defense was no longer a major priority for emergency planners or Congress. In March 1992, President Bush signed National Security Directive 66 instructing FEMA to develop a multi-hazard approach to emergency management

combining Civil Defense preparedness with natural and man-made disaster preparedness. Criticized for its poor response to the Exxon Valdez Oil Spill, Hurricane Hugo, and the Loma Prieta Earthquake, in November 1990 FEMA began work on developing a Federal Response Plan (FRP). Drawing from the Incident Command System and Incident Management System framework, the FRP defined how 27 Federal agencies and the American Red Cross would respond to the needs of State and Local governments when they were overwhelmed in a disaster. [58]

President Clinton oversaw the final dismantling of US Civil Defense with his appointment in 1993 of James Lee Witt as the new FEMA Administrator. His reorganization plan entitled "The Renewal of the Federal Emergency Management Agency" failed to mention Civil Defense even once in its 18 pages. His proposal subsumed Civil Defense programs into FEMA's all-hazards mission, which had become synonymous with natural disasters. While parts were repurposed from some of their Cold War duties, others including whole offices disappeared entirely. The last remnants of Civil Defense were buried within the bureaucracy of FEMA. The long running conflict over the allocation of resources between Civil Defense and natural disasters was over. [57] In November 1994, the Federal Civil Defense Act of 1950 was repealed and all remnants of Civil Defense authority transferred to Title VI of the Stafford Act. [58]

President George W. Bush had been in office eight months when the US was attacked on September 11, 2001. It was the first direct attack on the US since World War II. The devastation wrought on 9/11 bore eerie resemblance to Pearl Harbor. Nearly 3,000 dead and over $50 billion in damages.[8] Except the devastation inflicted on Pearl Harbor on December 7, 1941 required the combined might of six first-line aircraft carriers and 420 combat aircraft from the Imperial Japanese Navy. By comparison, the 9/11 attacks were executed by 19 terrorists who hijacked 4 passenger jets and turned them into guided missiles. It was a criminal act with national repercussions, what the 9/11 Commission Report called "disproportionate". It was an unprecedented application of force by non-state actors. It was met by an unprecedented re-organization of US government. In November 2002, President Bush signed the Homeland Security Act creating the Department of Homeland Security. The purpose of DHS was to "empower a single Cabinet official whose primary mission is to protect the American homeland from terrorism." The Secretary of Homeland Security would have authority over Federal resources to protect, prevent, respond, and recover from domestic catastrophe. FEMA would be a key component in the new organization. It was expected to reduce the loss of life and property and protect the nation's institutions from all types of hazards through a comprehensive, risk-based, all-hazards emergency management program of preparedness, mitigation, response, and recovery. [59]

Cold War to War on Terrorism

The US and Soviet Union were ideological competitors. The US stood for democracy and capitalism, the USSR stood for communism and authoritarianism. Based as it was in a country with a long and brutal history of being invaded, the Russian form of communism saw western democracy as a mortal threat that was best eliminated. In November 1956, Soviet First Secretary Nikita Khrushchev famously told a group of western ambassadors "We will bury you!"[9] Following the successful detonation of its first atomic bomb in August 1949, the Soviet Union aggressively pursued the

[8] The Japanese attack on Pearl Harbor killed 2,471 people and damaged or destroyed 19 US Navy ships including 8 battleships.

[9] Khrushchev made the statement while addressing Western ambassadors at the Polish Embassy in Moscow. Twelve envoys from NATO and Israel immediately departed, but modern translators have suggested the phrase was mistranslated or taken out of context.

acquisition of more and mightier weapons and the means to deliver them to the US. In November 1952, the USSR first flew the Tupolev Tu-95 (NATO call sign "Bear") bomber with a range of 5,000 miles capable of dropping an atomic bomb on the US. In November 1955, the Soviet Union detonated its first hydrogen bomb yielding 1.6 megatons of explosive force, more than 100 times that which destroyed Hiroshima Japan during World War II. And in October 1957 the USSR launched Sputnik 1, the first artificial Earth satellite carried into orbit atop a modified R-7 intercontinental ballistic missile. For forty-five years the US and USSR engaged in both direct and indirect global confrontation that at any minute threatened to turn the Cold War into World War III, some examples which include the 1948-49 Berlin Airlift, 1950-53 Korean War, 1961 Berlin Crisis, 1962 Cuban Missile Crisis, 1954-75 Vietnam War[10], and 1973 Yom Kippur War. By 1986, at the peak of the paranoia, the Soviet Union had amassed over 45,000 atomic warheads and the US some 24,000, more than enough to destroy the world many times over.[11] Since 1947 the Bulletin of Atomic Scientists has maintained the Doomsday Clock wherein the minutes or seconds before midnight are a metaphor for imminent danger to humanity. The clock's original setting in 1947 was seven minutes to midnight. It has since been set backward 8 times and forward 16 times. After the Soviet Union collapsed and the Cold War ended in December 1991, the Doomsday Clock was set to 17 minutes from midnight, its most distant point ever.

Although the world was safer, it was still far from safe. On August 2, 1990, Iraqi forces advanced south into Kuwait overrunning the country in two days and gaining possession of its oil fields, raising concerns in world markets. The US didn't depend on Persian Gulf oil but Europe and Asia did, and it was in US economic interests to stabilize the region for the sake of its major trading partners. Concerns that Iraqi forces might continue south into Saudi Arabia prompted the Kingdom to accept an offer of US military support. On August 7, 1990, the 82nd Airborne landed in Dhahran. Over the next four months the US forged an international coalition of 31 countries and led a rapid buildup of military force that was designated Operation Desert Shield. After diplomatic efforts failed to dislodge Iraq from Kuwait, the United Nations passed Resolution 678 authorizing the use of force. On January 16, 1991, the coalition launched Desert Storm. The coalition offensive began with a 42-day air campaign that quickly gained air supremacy before it began whittling away at Iraqi leadership, communications, and forces. On February 24, 1991, the ground campaign commenced when the 1st and 2nd Marine Divisions and 1st Light Army Infantry Battalion crossed into Kuwait and headed for Kuwait City. At the same time, the US VII Corps together with French and British armor divisions drove deep into Iraq then turned east and smashed into the flank of the elite Republican Guard. The Iraqis took heavy casualties before resistance crumbled and they began to surrender or retreat. Within 100 hours coalition ground forces overran the enemy and liberated Kuwait. An estimated 100,000 Iraqi soldiers died in the conflict. From the fruit of this victory, however, were sown the seeds of dissension that would grow and become an unprecedented new threat to the US. [1]

The seventeenth child of a Saudi construction magnate, in 1980 Osama bin Laden left university to fight the Soviets who invaded Afghanistan the previous December. Arriving in Pakistan, bin Laden used money and machinery from his own construction company to help the Mujahideen fight against

[10] Neither Korea nor Vietnam were declared US wars. Congress last declared war in World War II. Although Korea was called a "police action" and Vietnam is generally labeled a "conflict", the people who fought and died in these countries justifiably considered themselves at war.

[11] Even if your country was not attacked, it was thought that an all-out nuclear exchange between the US and USSR would inject so much fallout into the atmosphere as to blot out the sun and induce an extended "nuclear winter" that would destroy harvests around the globe.

the Soviet Army. By 1984, bin Laden and his partner had established al Qaeda to funnel money, arms, and fighters from around the Arab world into Afghanistan. After nine years, heavy losses, and no victory, the Soviets withdrew from Afghanistan in April 1988. In 1990 bin Laden returned home to Saudi Arabia. In August that year, Iraq invaded Kuwait. Concerned that Iraqi forces might continue south into Saudi Arabia, the Saudi monarchy accepted a US offer to deploy troops in defense of the Kingdom. On August 7, 1990, the 82nd Airborne landed in Dhahran and took up border defensive positions. Osama bin Laden was outraged by this apparent infidel incursion onto holy Muslim territory. Saudi Arabia is home to the two holiest sites in Islam: Mecca and Medina. Bin Laden's denouncements resulted in government censure and caused him to flee to Sudan. Bin Laden was welcomed to Sudan by the head of the National Islamic Front. He used his family fortune and construction company to assist with building a road from Khartoum to Port Sudan. Bin Laden also used his contacts to acquire weapons and explosives for terrorist purposes. During this time, al Qaeda was suspected of supporting attacks against US forces in Yemen, Somalia, and Saudi Arabia, and attempting to assassinate the President of Egypt. Under pressure from the US, bin Laden was expelled from Sudan. Because his Saudi Passport was rescinded, he made his way back to Afghanistan where he lent his support to the ruling Taliban. After the coalition forced Iraq out of Kuwait in February 1991, US forces remained in Saudi Arabia to protect the Kingdom from any further aggression by Saddam Hussein. After arriving in Afghanistan in 1996, bin Laden issued a religious edict declaring war on the US. In August 1998, al Qaeda detonated two truck bombs outside US embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, killing 224 people and injuring 4500 more. In October 2000, al Qaeda rammed a speed boat loaded with explosives into the destroyer USS Cole while at port in Yemen, killing 17 sailors. Although bin Laden and al Qaeda had come to the attention of the White House and ways had been considered to kidnap or kill him, both the CIA and Pentagon thought the risks disproportionate. Meanwhile, Khalid Sheikh Mohammed, one of bin Laden's commanders, came to him with a plan. KSM proposed several options for directly attacking the US. One plan called for hijacking ten aircraft and crashing them into the Twin Towers, Pentagon, White House, CIA and FBI headquarters, several nuclear power plants, and the tallest buildings in California and Washington state. Bin Laden was noncommittal. At the time he was busy with other plans. But about April 1999, bin Laden summoned KSM and told him al Qaeda would support his plan, but he had to scale it back. KSM agreed to four targets: the Twin Towers, Pentagon, White House, and US Capitol. It was called the "Planes Operation". [60]

Homeland Security arose in 1995 out of renewed concerns about direct attacks on US territory and population. Homeland Security came to the attention of the US government as a result of the 1995 Tokyo Subway Attacks. It was the first time a weapon of mass destruction (WMD) was employed by a non-state actor. The term weapon of mass destruction is loosely defined in Title 18 Section 2332a United States Code (USC) as Chemical, Biological, Radiological, and Nuclear (CBRN) devices capable of causing large-scale death and/or destruction. Prior to the Tokyo Subway Attacks, it was thought only nation states could afford the means to fabricate WMD. In 1995 a quasi-religious cult, Aum Shinrikyo successfully synthesized liquid Sarin. An odorless, colorless liquid, Sarin is a nerve agent that quickly vaporizes when exposed to air. Highly potent, a single drop can kill a grown adult. On March 20, 1995, cult members entered the Tokyo subway system and boarded separate trains bound for the city center, the seat of Japanese government. Each carried two plastic bags filled with liquid Sarin and an umbrella with a sharpened tip. As the trains drew near the city center, the cult members dropped their bags to the floor and punctured them with their umbrellas. As the Sarin started vaporizing, passengers within the packed cars began to fall sick. Victims would later report feeling nauseous and having blurred vision.

As the trains pulled into the next station, passengers rushed out of the cars, unwittingly spreading the Sarin onto the platform. Soon, waiting commuters also began feeling the effects and started pushing towards the station exits. Some collapsed on the platform before they could make it. Seeing the pandemonium, subway agents ordered all trains stopped but not before thousands were exposed. Hundreds collapsed outside the station entrances. Over 5,000 made their way to hospitals, overwhelming staff who were unsure what was happening. Miraculously most victims survived. Unfortunately, twelve did not. Experts believe thousands more could have died. Japanese police traced the attacks back to the cult leader Shoko Asahara. He staged the attacks to bring down the Japanese government and hasten a prophesized global apocalypse from which he would emerge as "emperor". After a lengthy trial, Asahara was convicted of murder and sentenced to death together with twelve other cult members. Asahara was executed by hanging on July 6, 2018. [1]

The Tokyo Subway Attacks demonstrated the ability of a small group of well-resourced and committed individuals to manufacture and deliver a weapon of mass destruction. The question arose in the United States: "What if it's not just them?" Less than a month after the Tokyo Subway Attacks, on April 19th, 1995, a van filled with ammonia fertilizer was exploded in front of a Federal building in downtown Oklahoma City, killing 168 people. The bombing was an act of terrorism. Timothy McVeigh, the instigator, had staged the bombing in retaliation for previous Federal raids on private compounds in Ruby Ridge ID, and Waco TX. Prior to that, in February 1993 a truck bomb was detonated inside the parking garage of the World Trade Center North Tower in New York City. Only six people died, but the attack was meant to topple the tower and kill thousands. Again, it was an act of terrorism. Ramzi Yousef, a Kuwaiti living in America, directed the attacks in retaliation for US foreign policy which he considered oppressive to Muslims in the Middle East. Both the Congress and White House worried: "What if terrorists tried to employ WMD inside the US?" Nations possessing WMD is one thing, non-state actors possessing WMD is another. Nations are known quantities, criminals aren't. Nations can be deterred, criminals not so much. As a result, both Congress and the White House chartered commissions to look into the matter. The Gilmore Commission, Hart-Rudman Commission, Bremer Commission, and other commissions all came back with the same answer: There was a basic lack of coordination between government branches needed to stop criminal acts with national consequences. In April 2001, Rep. William Thornberry (R-TX) introduced HR 1158 proposing a National Homeland Security Agency to provide the government coordination needed to thwart the criminal WMD threat. The bill was still sitting in Congress five months later when 9/11 occurred. [60]

9/11 brought homeland security to the forefront of US policy concerns. Because both the Tokyo Subway Attacks were terrorist acts, homeland security was defined in terms of terrorism:

> *"Homeland Security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur." - 2002 National Strategy for Homeland Security*

The definition was somewhat misleading. It contended that terrorism was the problem. According to Title 18 Section 2331 USC, terrorism is a crime distinguished by motive, namely to coerce US government. Terrorism was not the problem. Terrorism had been a national concern since the mid-nineteenth century. If it was the problem it would've been addressed much earlier. The problem was WMD wielded by non-state actors. That was new, as demonstrated by the Tokyo Subway Attacks. And though the 9/11 hijackers did not employ WMD themselves, they achieved WMD effects by subverting

the nation's transportation infrastructure. Be that as it may, both groups harbored terrorist motives intending to coerce their targeted governments: Aum Shinrikyo wanted to overthrow Japanese government to precipitate an apocalypse; al Qaeda wanted to force the withdraw of US troops from Saudi Arabia. Somehow "WMD wielded by non-state actors" became conflated into "terrorism" and set the new Department of Homeland Security on a collision course with disaster.

The Global War on Terrorism (GWOT) began October 7, 2001, when the US attacked Afghanistan on its hunt for Osama bin Laden. A cross check of the 9/11 flight manifests implicated al Qaeda in the attacks. Osama bin Laden was known to be in Afghanistan, protected by the Taliban government. The National Security Council spent the next ten days preparing diplomatic and military options. On September 22, in a speech before Congress, President Bush sent an ultimatum to the Taliban: Give up al Qaeda or share their fate. "Either you are with us, or you are with the terrorists." The Taliban refused to give up bin Laden. On October 7, the US launched Operation Enduring Freedom to remove the Taliban, eliminate al Qaeda, and capture or kill Osama bin Laden. CIA units infiltrated Afghanistan and joined up with the Northern Alliance, enemies of the Taliban. Supported by special operations ground forces and US airpower, they began their campaign. With US military backing, the Northern Alliance advanced on the Afghan capital of Kabul. On November 9 they took Mazar-i-Sharif, after which a cascade of provinces fell with minimal resistance. On November 12, the Taliban gave up Kabul and began to retreat south. The Northern Alliance continued in pursuit. Finally, in early December the Taliban gave up Kandahar, their last stronghold. In two months the Taliban were swept from power and an Islamic Republic set up in their place. But al Qaeda forces continued to fight from the caves of Tora Bora where bin Laden was last seen. A military push the following March succeeded in shutting down al Qaeda, but bin Laden escaped. The FBI issued a $25 million bounty for information leading to bin Laden's capture. When nobody came forward to claim the reward, some thought he must be dead. After bin Laden fled Tora Bora in 2002, numerous speculative press reports placed him in various locations. Pakistan was regularly identified as a suspected hiding place. In April 2011, US intelligence began to suspect bin Laden was in Abbottabad. Agents eventually pinpointed his home to a three-story mansion only a mile away from the Pakistan Military Academy. On April 29, 2011, President Obama authorized a team of Navy SEALs to raid the compound. Without consulting Pakistan, on May 2, 2011, stealth helicopters flew the SEALs into Abbottabad. One helicopter crash landed inside the compound. The other landed outside the wall. Nobody was seriously injured. The wall was breached and the teams advanced together towards the house. They broke in and made their way upstairs. They wore night vision goggles to see in the pitch dark. Bin Laden peered from his door. The SEALs fired, then leapt into his room and shot twice again. The SEALs reported "Geronimo, Geronimo, Geronimo", confirming that bin Laden was killed. The SEALs evacuated the body with them back to Afghanistan. There, it was flown to the carrier Carl Vinson. After final confirmation of identity, religious rites were performed and the body buried at sea. [1]

Osama bin Laden declared war against the US because our forces were stationed in Saudi Arabia, home to the two holiest shrines in Islam, Mecca and Medina. The stationing of US forces in Saudi Arabia was an affront to many Muslims. The only way to prevent the situation from becoming a pretext for another 9/11 was to remove them. The only thing standing in the way of a US withdraw from Saudi Arabia was Saddam Hussein. Saddam Hussein was the brutal dictator of Iraq. In 1979 he took control of Iraq by having all his political opponents killed. Over the next 24 years he killed thousands: enemies, friends, family, and countrymen. In September 1980 he invaded Iran. The attack quickly ground to a halt. Both sides took up defensive lines and began pounding each other's positions. It became a bloody war of attrition. The conflict resembled World War I in terms of large-scale trench warfare with bayonet

attacks by human waves against machine guns behind barbed wire, and extensive use of chemical weapons. Mustard gas was used to halt Iranian advances on the front and punish Kurdish rebels in Iraq. After eight bloody years, the war ended in stalemate. An estimated half-million soldiers died. Iraq came out of the war heavily in debt. It owed $30 billion to its wealthy neighbor Kuwait. Kuwait refused to forgive Iraq's debt. Saddam Hussein also accused them of stealing Iraq's oil. To eliminate Iraq's debt to Kuwait, Saddam Hussein decided to eliminate Kuwait. Although Saddam Hussein lost the war, he still remained in power. He now turned his attention to crushing the rebellions trying to topple him. He sent his remaining forces to crush the uprising of ethnic Kurds in the north, and Shia Muslims in the south. Tens of thousands of Iraqi people were killed before the coalition intervened. Coalition forces established military exclusion zones to keep Iraqi forces out of northern and southern Iraq. These were enforced by US and allied forces based in Turkey and Saudi Arabia. US forces also remained in Saudi Arabia to deter Saddam Hussein from again attacking south. It was because US forces remained in Saudi Arabia that Osama bin Laden declared war in 1996. After removing the Taliban and al Qaeda from Afghanistan in 2002, the US turned to Iraq. On March 20, 2003, the US, again at the head of a coalition, launched Operation Iraqi Freedom. The combined air and ground campaign lasted only six weeks before Baghdad was taken. Within days, US forces began pulling out of Saudi Arabia and our visible military presence is now gone. Saddam Hussein fled into hiding but was found and captured nine months later. Three years after that he was tried and sentenced for crimes against humanity. On December 30, 2006, he was hanged. [1]

The death of Osama bin Laden in 2011 did not end the threat of terrorism to the US. After US forces overran Afghanistan and Iraq, both countries disintegrated into competing hostile factions and were overcome with internal strife. Al Qaeda and Taliban rebels maintained footholds in Afghanistan, and a brutal new terrorist group proclaiming itself the Islamic State took hold in parts of Iraq and Syria. US forces remained to support the fledgling democracies in both countries and prevent them from becoming safe havens for terrorists as Afghanistan had been for al Qaeda under the Taliban. US forces withdrew from Iraq in 2011, perhaps a little prematurely, but the rule of law and democracy continued to prevail. By 2021 the US had been conducting combat operations in Afghanistan for 20 years and it had eclipsed Vietnam as the longest war in US history.[12] In August 2021 US forces were making a peaceful withdraw when a resurgent Taliban violently overthrew the democratic government and seized control of Afghanistan. As they struggle to reassert control over their country, the Taliban do not pose a threat to the US, nor do the remnants of Islamic State in Syria. Indeed, despite the setbacks, US military operations conducted over the past twenty years have succeeded in their goal. The US has not suffered another 9/11-type attack in all that time. That does not mean the US is invulnerable.

Civil Defense to Emergency Preparedness

At no time during the Cold War was the US or its population directly attacked, but if the Cold War had turned hot, the entire nation was under threat of unprecedented devastation. After the Cold War the US and its population suffered from unprecedented direct attack, but at no time during the Global War on Terrorism was the entire nation under threat of devastation. Perhaps most ironically, the conflict for dual-use Civil Defense spending settled in 1993 in favor of "natural disasters" reverted back to "military attack" when FEMA merged into DHS in 2002. That singular focus was shattered when Hurricane Katrina slammed into the Gulf Coast in August 2005.

[12] US military operations in Vietnam lasted 19 years from 1954 to 1973.

The tropical depression that became Hurricane Katrina formed over the Bahamas on August 23rd, 2005. By August 26th, after crossing Florida into the Gulf, it had become a Category 5 storm. Katrina's high winds and floods severely damaged the Gulf coast from Florida to Texas. Florida was hit twice when Katrina crossed the tip on August 25th and grazed the panhandle on August 29th. Alabama and Mississippi also sustained heavy damage; 238 were killed, and 900,000 lost power. They might have become the center of national attention except for what happened in New Orleans. On August 29th, Hurricane Katrina made second landfall near Buras-Triumph Louisiana and headed inland towards New Orleans packing 125 mph winds, a 14-foot storm surge, and 8-10 inches of rain. The rain overflowed Lake Pontchartrain, causing flooding along its shores. Several bridges were destroyed, including the I-10 Twin Span Bridge, and most roads in and out of the city were damaged. Power went out. High rise windows were shattered. And the Superdome roof was peeled. However, by mid-day as the eye passed to the east, it seemed the city had been spared the worst. But then the levees began to break. Katrina's storm surge overwhelmed the city's levees and drainage canals. The Mississippi River Gulf Outlet breached its levees in 20 places. The federally built levee system protecting downtown New Orleans breached in 53 places. New Orleans began to flood. By August 31st, 80% of the city was flooded, some parts 15-feet deep. The extensive flooding stranded many residents in their homes. Many chopped their way onto their roofs. Some were trapped inside their attics. Without food, power, or water, they waited for rescue. The first deaths were reported shortly after midnight on August 28th. Three nursing home patients died during an evacuation to Baton Rouge. By 11:00 pm on the 29th, Mayor Nagin described the loss of life as "significant", noting reports of bodies floating on the water throughout the city. Reports of rioting and looting prompted the Mayor to impose a curfew August 31st. Governor Blanco ordered in 6500 National Guard to help maintain order. The situation at the Superdome was dire. A designated storm shelter, it had insufficient food, water, and facilities for all the people who flocked to its doors. The same was true at the Convention Center. People stranded at home and in shelters suffered and waited for help that was slow to arrive. New Orleans Fire Departments didn't have the buses or boats needed for the massive rescue operation. New Orleans Police were short-handed due to desertions within the ranks. Coordination among rescuers was poor due to incompatible radios and inadequate direction. Few were knowledgeable on the City's emergency management procedures. As the National Guard began to arrive in force, more people were rescued and evacuated to safety. By September 3rd, the Superdome and Convention Center were emptied. On September 4th, 16,000 National Guard troops swept the city searching for remaining victims. About 2,000 people with serious medical conditions were treated at Louis Armstrong Airport. FEMA officials arranged for additional rescue units and helped supply food, shelter, and medicine. Later, active duty military forces arrived and lent their support to the National Guard. Hurricane Katrina constituted the largest deployment of military forces within the US since the Civil War. Sadly, 1,464 Louisiana citizens lost their lives to Hurricane Katrina. Investigations following the hurricane decried many of the deaths as "preventable". Furthermore, they determined that the suffering in the days and weeks after the storm were unnecessarily prolonged. Government at all levels had failed to plan, prepare, and respond aggressively to the storm. Primary blame fell on FEMA. Its focus on terrorism had detracted from emergency management. As a result, both FEMA and the Department of Homeland Security were overhauled and their missions broadened to encompass "All Hazards". [61]

The nation's First Responders,[13] supported as they are by State and Local taxes do not report to the Federal Government. FEMA can direct nothing, however, it can influence a lot. FEMA is empowered by the Homeland Security Grant Program (HSGP) to elicit voluntary cooperation and develop standards across State and Local First Responder agencies. In 2004 FEMA made adoption of the National Incident Management System (NIMS) a prerequisite for HSGP funding. NIMS offered the organizational construct of the Incident Command System (ICS) for integrating response assets across State, Local, and Federal jurisdictions, and orienting them towards common objectives identified in an Incident Action Plan promulgated by the local Incident Commander. State and Local jurisdictions were also encouraged to develop Mutual Aid Agreements and help each other to the maximum extent possible before seeking Federal support. However, if Federal support became necessary, FEMA provided the means for requesting it using the National Response Framewok (NRF). The NRF was the successor to the NRP which originated with the FRP. Criticism following FEMA's response to Hurricane Hugo in 1989 prompted the agency in 1992 to develop a comprehensive Federal Response Plan. After FEMA was incorporated into DHS in 2002, the FRP was replaced in 2004 by the National Response Plan (NRP). The 2004 National Response Plan stipulated the mechanisms for requesting Federal support in accordance with the 1988 Robert T. Stafford Act and provided a compact means for delivering requested support in the form of Emergency Support Functions (ESFs). The ink had barely dried on the NRP when Hurricane Katrina hit in 2005. The ensuing confusion prompted a rewrite of the plan in the form of the 2008 National Response Framework. The NRF remains the basis for preparing and responding to "All Hazard" disasters across Federal, State, Local, Tribal, and Territorial governments. [62]

The NRF is predicated on a bottom-up process for requesting additional resources only when all local capability is overwhelmed or exhausted. States have significant resources at their disposal in the form of firefighters, police, paramedics, and the National Guard. A standing Emergency Management Assistance Compact (EMAC) allows Governors to request additional National Guard support from other States. Federal assistance can only be made available after a Governor declares a State disaster or emergency and submits a request for assistance to the President. This process is mandated by the Stafford Act and is designed to respect the sovereignty of States as stipulated in the Tenth Amendment to the Constitution. Once the President approves a Governor's request, FEMA is given responsibility for coordinating the Federal response and delivering ESF support to the States. Various Federal agencies are assigned primary and supporting roles in delivering ESF capabilities. As a support agency for all ESFs, the Department of Defense stands responsible for lending Defense Support of Civil Authorities (DSCA) when requested. Under exceptional circumstances, the President may pre-position Federal support in advance of an expected disaster, as was the case with Hurricane Sandy in 2012. Otherwise, the Department of Homeland Security will deploy a Federal Coordinating Officer (FCO) to advise the State Coordinating Officer in preparing and submitting individual Requests for Assistance. Deployed Federal assets establish a base of operations and conduct missions as assigned by the Incident Commander. State and Local officials retain control over all response and recovery operations. Of course, Federal assistance doesn't come free. In accordance with the Stafford Act, State and Local governments are committed to reimbursing the Federal government up to 25%, and possibly more of the total costs. This provision is designed to keep States responsible for their own disasters and avoid the moral hazard of depending too much on Federal support. In fact, FEMA maintains a National Preparedness Goal (NPG) identifying 32 Core Capabilities necessary to become self-proficient in any disaster. Again, using Homeland Security

[13] The term "First Responders" generally refers to those who are first on-scene in an emergency and include law enforcement, firefighters, and emergency medical personnel.

Grant Program funding, FEMA is trying to guide State and Local investments towards building Core Capabilities that will decrease their dependence on Federal assistance. Towards this end, all HSGP recipients are required to conduct an annual Stakeholder Preparedness Review (SPR) and update their Threat and Hazard Identification and Risk Assessment (THIRA) every three years. [62]

HSGP, NIMS, and NRF are generally considered successful programs and largely credited for improving the nation's readiness to respond to natural disasters. Indeed, the US has become quite proficient at responding to severe hurricanes as their number and frequency have increased due to effects from global climate change. However, the consequences from even the worst hurricane is confined regionally to perhaps a handful of States. The same is true for other probable large-scale natural disasters[14] like earthquakes, volcanoes, and tsunamis. Although the potential devastation is incalculable, it will still be regionally confined to perhaps a handful of States. The distinction is significant because it means there will be equally large portions of the US unaffected by the disaster from which a viable response can be mounted. The NRF will still work as designed and help will be promptly forthcoming. But what happens if the consequences from disaster are nationwide? What happens if everybody is affected and nobody is available to lend help? How do we respond to disaster when the devastation is nationwide?

21st Century Civil Defense Authorities

After the end of the Cold War, Civil Defense was all but replaced by Emergency Preparedness, the basic difference of which is scope. Civil Defense prepared for a nationwide disaster whereas Emergency Preparedness mainly prepares and responds to regional disasters, whether natural or manmade. Then in 2010, the Quadrennial Homeland Security Review raised the prospect of a nationwide disaster brought about by cyber-attack on the US electric grid. Russia, China, and North Korea had the means and opportunity to mount such a cyber-attack, but the motive was generally lacking. That changed when Russia invaded Ukraine in February 2022. President Putin publicly threatened to retaliate against the US if he felt Russia was under attack. That threat specifically invoked a nuclear option but also implied cyber-attack which Russia was employing in full force against Ukraine. China took advantage of the situation to press its claims on Taiwan and North Korea accelerated its nuclear missile program, either of which could also lead to direct confrontation with the US. The confluence of means, opportunity, and now motive suggest that it would be prudent to resurrect US Civil Defense programs. As Mr. Lucie correctly points out, remaining Civil Defense authorities survive in Title 50, Section 3042 USC as follows:

> *It shall be the function of the Administrator of FEMA to advise the President concerning the coordination of military, industrial, and civilian mobilization, including—*
>
> *(1) policies concerning industrial and civilian mobilization in order to assure the most effective mobilization and maximum utilization of the Nation's manpower in the event of war;*

[14] We do not consider "black swan" low-frequency high-consequence natural disasters such as asteroid strike and super-volcanoes because they are probable extinction events from which nations will inconceivably survive.

(2) programs for the effective use in time of war of the Nation's natural and industrial resources for military and civilian needs, for the maintenance and stabilization of the civilian economy in time of war, and for the adjustment of such economy to war needs and conditions;

(3) policies for unifying, in time of war, the activities of Federal agencies and departments engaged in or concerned with production, procurement, distribution, or transportation of military or civilian supplies, materials, and products;

(4) the relationship between potential supplies of, and potential requirements for, manpower, resources, and productive facilities in time of war;

(5) policies for establishing adequate reserves of strategic and critical material, and for the conservation of these reserves;

(6) the strategic relocation of industries, services, government, and economic activities, the continuous operation of which is essential to the Nation's security.

In performing his functions, the Administrator of FEMA shall utilize to the maximum extent the facilities and resources of the departments and agencies of the Government.

What CD Authorities Do

Title 50 Section 3042 USC authorizes FEMA to direct and coordinate Civil Defense preparedness and response activities within the scope of its legally constituted organizational jurisdiction.

As it does today, FEMA assists State and Local governments with developing and enhancing emergency preparedness through grants administered under HSGP and directed by THIRA/SPR. Likewise, FEMA response is authorized under the 1988 Stafford Act, governed by the 2019 National Response Framework, and accomplished according to the latest National Incident Management System.

What CD Authorities Don't Do

Title 50 Section 3042 USC DOESN'T give FEMA authority to override Federal, State, or Local government in directing and coordinating Civil Defense preparedness and response activities.

Just as the FEMA Administrator doesn't direct emergency preparedness and response, at no point are they authorized to take control of CD activities. As with emergency preparedness, all CD activities will be conducted by legally authorized Federal, State, Local, Tribal, and Territorial government officials. Certainly, as they do today the FEMA Administrator may advise the President and National Security Advisor, but that does not translate into directive authority outside the FEMA organization. Similarly, FEMA may request support from other executive agencies, but it cannot direct it.

What CD Authorities Imply

Civil Defense authorities delegated to FEMA under Title 50 Section 3042 USC imply that US government must survive and have the means to effectively govern.

As it was during the Cold War so it remains that Continuity of Government (COG) and Continuity of Operations (COOP) are priority Civil Defense objectives. COOP ensures an individual organization can continue to perform its essential functions providing essential services and delivering core capabilities

following disaster. COG is a coordinated effort to ensure that governance and essential functions continue to be performed before, during, and after an emergency. COOP and COG collectively provide Enduring Constitutional Government (ECG) capable of delivering National Essential Functions (NEFs). [63]

NEF 1: Preserve Our Constitutional Government	NEF 5: Protect the Homeland
NEF 2: Provide Visible Leadership	NEF 6: Provide Emergency Response/Recovery
NEF 3: Defend the Country	NEF 7: Maintain a Stable Economy
NEF 4: Maintain Foreign Relations	NEF 8: Provide Critical Government Services

Table 2: National Essential Functions, 2018 FEMA Continuity Guide

What CD Authorities Don't Imply

Civil Defense authorities delegated to FEMA under Title 50 Section 3042 DON'T imply that US government will forsake the Constitution or the protections it affords the governed.

CD authorities don't automatically assume civil rights will be suspended in the face of a nationwide attack. Accordingly, CD preparedness and response activities must maintain constitutional protections for life, liberty, and property. Just as FEMA can't direct what it doesn't directly control, the same is true with US government. It cannot dictate to private citizens or businesses how they will conduct themselves or manage their property.

What CD Actions Are Likely

As it was during the Cold War and remains today, FEMA WILL likely assist State and Local governments with Civil Defense preparedness and response activities.

As it has done with natural disasters, FEMA may work in partnership with Federal, State, Local, Tribal, and Territorial governments to develop plans, exercises, and measures to mitigate the effects and quickly recover from catastrophic attack. FEMA's program of continual improvement is designated the National Preparedness Goal.

What CD Actions Aren't Likely

As it was during the Cold War and remains similar today, FEMA ISN'T likely to oversee a prohibitively expensive CD program that doesn't have American public support.

Public support is essential to gaining Congressional funding for CD programs. During the Cold War, Congress supported dual-use programs that benefitted both Civil Defense and Emergency Preparedness.

Revitalizing 21st Century Civil Defense

Writing as he did in 2017, before the resurgence of a nuclear threat to the US, Mr. Lucie smartly determined that "A 21st century Civil Defense program must be prepared to meet old threats while recognizing the need to meet new ones." As he saw it, "The threat of nuclear attacks upon the United States still exists, along with a renewed ability of potential adversaries to attack the United States directly through military strikes and sabotage. In addition, new forms of asymmetric warfare have developed since the termination of the Civil Defense program in 1993, including the use of the internet and social media to attack critical infrastructure and the American economy directly and to influence or even directly attack elections. This program would also seek to continue to maximize its dual-use nature,

developing capabilities that could also be used for natural and man-made disasters not related to war." Accordingly, Mr. Lucie suggested three priorities for a revitalized Civil Defense Program:

1. Protect the population, defense base, critical infrastructure, and preserve government.
2. Support DOD efforts to deploy military capabilities while under attack.
3. Mobilize and sustain the nation's defense and manpower base. [57]

Mr. Lucie frames these priorities under the assumption that "the primary purpose of a revitalized Civil Defense program would be to support the Nation's war time efforts and not as another division supporting catastrophic planning." Like Pearl Harbor in 1941, he believes that a direct attack on the US would be the opening salvo of a protracted military campaign against the nation or its interests. As he puts it, "This new program must be prepared to support the Nation's efforts to fight a war on simultaneous fronts. These fronts include the location of one or more overseas contests between armies, the physical defense of the homeland, sustaining and expanding the domestic critical infrastructure supporting both military needs and the civilian economy, the defense of our political institutions from foreign interference, and the preservation of national morale. The government must be prepared to see these fronts under attack from combined efforts both conventional and asymmetric, and not assume future enemies will require the use of nuclear weapons to carry out these attacks." [57]

Certainly, the presiding Civil Defense authorities in Title 50 Section 3042 USC support this scenario, but is it probable? There's an aphorism well known in military circles that we often prepare for the next war assuming it will be like the last war.[15] Thus the investigating committee characterized 9/11 as a "Failure of imagination" when F-16 fighters were launched out over the Atlantic to intercept Russian bombers instead of being vectored against passenger jets in New York.[16] [60] Originating as they did in 1950, the presiding Civil Defense authorities are heavily influenced by the US military experience in World War II where indeed after an initial debilitating blow, the nation mustered its immense industrial capacity to deploy and support overwhelming military force in Europe and the Pacific. It would seem unlikely given something like the preceding Ukraine Nuclear Scenario, but certainly possible after a Black Sky Event instigated by other means.

Perhaps more interesting is the observation that Mr. Lucie's recommendations contain a dependent relationship whereby the last two priorities depend on the first. If you can't ensure the first, then you can't ensure the second or third. The problem is we can't ensure Mr. Lucie's first priority. We have neither the means nor ability to protect critical infrastructure.

EP Programs & Objectives

Critical infrastructure is the "Achilles Heel" of contemporary urban civilization. Without it, urban society would break apart, yet very little of it was designed to withstand deliberate attack. This proved devastating on 9/11 when criminals exploited vulnerabilities in the US transportation infrastructure created WMD effects by turning passenger jets into guided missiles. The realization that US critical

[15] The source of this saying is lost to history, but a modern form of it is attributed to J. L. Schley, Lt. Col. US Army who wrote in 1929 "It has been said critically that there is a tendency in many armies to spend the peace time studying how to fight the last war."

[16] NORAD air defenses completely failed on 9/11, however, even if F-16 fighters had been vectored to New York, they wouldn't have arrived in time to intercept, and it's questionable they could have fired on passenger jets.

infrastructure could become the target of asymmetric attack dates back before 9/11 and forms the foundation for much of today's Emergency Preparedness programs and objectives.

Following the 1995 Tokyo Subway Attacks, President Clinton commissioned a panel to examine the vulnerability of US critical infrastructure to similar attack. The first executive guidance on critical infrastructure protection was PDD-63 issued in 1998. The guidance came too little too late and was unable to protect the transportation sector on 9/11. However, PDD-63 became the blueprint for the DHS National Infrastructure Protection Plan (NIPP). Although the plan has been revised, it remains basically the same as when first issued in 2006. The plan is comprised of two parts: 1) an organization, and 2) a process. The organization is comprised of Sector Coordinating Councils, one for each infrastructure sector. Each SCC is made up of government and industry representatives. Their purpose is to collect information, analyze data, and share insights on how to protect their different sectors. Each sector is guided by a process called the Risk Management Framework (RMF). The RMF is a continuous improvement process that begins by identifying critical infrastructure. The RMF then steps infrastructure owners through a process of identifying protective measures, performing cost-benefit analysis to select measures, implementing measures, then analyzing results. It sounds very simple and straight forward, but it's not. Security costs money and eats into profits. DHS Homeland Security Grant Programs can't pay industry for protective improvements. Even so, all the protective improvements in the world can't stop a determined attacker. Hardening and redundancy can be overcome because attackers have the advantage of time to seek out and exploit vulnerabilities. Just as there is no perfect defense, there is no absolute security. Everything is risk management. Why do we have door locks? They won't stop a determined attacker. But they still have deterrent value. They discourage the opportunistic thief and keep honest people honest. Same with airport security, or any other kind of security.

The Disaster Management Cycle originated in the 1970s as a means to help plan for and reduce the consequences of disasters. The cycle has undergone many permutations since it was first introduced in 1975, but today's generally accepted version includes four phases to any disaster: Prevent, Protect, Respond, and Recover. [64] The first two phases generally constitute what is called "preparedness" before a disaster strikes. The second two phases generally constitute what are called the "consequences" after a disaster strikes. Mitigation is sometimes identified as the fifth phase of disaster, but in reality occurs across all four phases as a means of reducing consequences. Mitigation done during preparedness can greatly reduce the magnitude and duration of consequences, which is why the old adage holds true that an ounce of prevention is worth a pound of cure. Ideally, mitigation measures that help avoid disaster are best because they eliminate all consequences. But some disasters just can't be avoided, like hurricanes, earthquakes, and determined attackers. Accordingly, the next best mitigation measures are those that best reduce the magnitude and duration of consequences. The difference in expected consequences from applying and not applying mitigating measures is a gauge of "resilience". The smaller the consequences, the greater the resilience.

National Preparedness Goal

Resilience is central to FEMA's National Preparedness Goal (NPG). The NPG was established by Homeland Security Presidential Directive #8 (HSPD-8) in December 2003 to guide Federal, State, Local, Tribal, and Territorial governments in developing capabilities making them more independent and resilient to disasters.

"A secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk." – 2016 National Preparedness Goal

The National Preparedness Goal establishes generally defined target capabilities as they apply across the different phases of the Disaster Management Cycle, including a Mitigation phase. It remains for agencies, officials, and stakeholders at each level of government to determine how those target capabilities specifically apply within their communities. To help them with their assessment, the NPG includes five supporting National Planning Frameworks (NPFs) providing high-level guidance on how to attain core capabilities associated with each of the recognized disaster phases. A corresponding set of five Federal Interagency Operational Plans (FIOPs) describe how the Federal government aligns resources and delivers core capabilities to support the National Planning Frameworks. [65]

Core Capability	P	P	M	R	R	Core Capability	P	P	M	R	R
1. Planning	X	X	X	X	X	17. Infrastructure Systems				X	X
2. Public Information & Warning	X	X	X	X	X	18. Critical Transportation				X	
3. Operational Coordination	X	X	X	X	X	19. Environmental Response/Health & Safety				X	
4. Intelligence & Information Sharing	X	X				20. Facility Management Services				X	
5. Interdiction & Disruption	X	X				21. Fire Management & Suppression				X	
6. Screening, Search, & Detection	X	X				22. Logistics & Supply Chain Management				X	
7. Forensics & Attribution	X					23. Mass Care Services				X	
8. Access Control & Identity Verification		X				24. Mass Search & Rescue Operations				X	
9. Cybersecurity		X				25. On-Scene Security, Protection, and Law Enforcement				X	
10. Physical Protective Measures		X				26. Operational Communications				X	
11. Management for Protection Programs & Activities		X				27. Public Health, Healthcare, & Emergency Medical				X	
12. Supply chain Integrity & Security		X				28. Situational Assessment				X	
13. Community Resilience			X			29. Economic Recovery					X
14. Long-Term Vulnerability Reduction			X			30. Health & Social Services					X
15. Risk & Disaster Resilience Assessment			X			31. Housing					X
16. Threats & Hazards Identification			X			32. Natural & Cultural Resources					X

Table 3: FEMA Core Capabilities, 2015 Emergency Preparedness Goal

The National Disaster Recovery Framework (NDRF) is one of the five National Planning Frameworks. The NDRF addresses the recovery phase of disaster management. The NDRF recognizes that recovery is not distinct but overlaps with the response phase of disaster management. Moreover, recovery planning during the preparedness phase is essential to developing the necessary capabilities to rapidly recover after disaster strikes. The NDRF basically advocates a vertical approach to planning that includes all agencies, officials, and stakeholders at each level of government. The purpose of the planning is to identify the necessary requirements to develop or strengthen the following Core Capabilities:

1. CC02 Public Information & Warning
2. CC03 Operational Coordination
3. CC17 Infrastructure Systems (Recovery)
4. CC29 Economic Recovery
5. CC30 Health & Social Services (Restoration)
6. CC31 Housing
7. CC32 Natural & Cultural Resources (Preservation) [66]

As its name implies, the NDRF is an over-arching framework offering strategy and doctrine for community disaster planning, meaning it is sparse on details. To further assist Federal, State, Local,

Tribal, and Territorial governments with disaster recovery planning, FEMA also offers various incident-specific guides. The 2017 FEMA Power Outage Annex provides detailed insight into the organization, operation, and authorities of the North American Electric Grid. The 2016 Incident Annex for Nuclear/Radiological Incidents, 2018 [Government] Continuity Guidance Circular, and 2021 Federal Support Annex for Evacuations provide similar details within their respective topics. The NDRF also suggests other resources including the FEMA website READY.GOV where under the "Disasters and Emergencies" tab can be found the "Recovering from Disaster" page, on which can be found a link to "Radiation Emergencies", on which page they have information about sheltering from radiation. These can be good resources when conducting community disaster planning.

Community disaster planning is facilitated by the National Preparedness System (NPS). The NPS is described in the 2018 FEMA Comprehensive Preparedness Guide (CPG-201) which also explains THIRA/SPR. Starting in 2012 States were required to submit an annual Threat and Hazard Identification and Risk Assessment (THIRA) in order to qualify for FEMA homeland security grants. Due to their involved nature, in 2018 THIRA's were extended to every three years, supplemented annually by a more abbreviated Stakeholder Preparedness Review (SPR). THIRA/SPR require States to justify their homeland security grants in terms of progress towards attaining National Preparedness Goal Core Capabilities. That progress is supported by the continuous improvement cycle of the National Preparedness System.

The NPS is a continuous improvement cycle comprised of the six steps listed in Table 4. THIRA/SPR is designed to establish a community's current capacity and proficiency with respect to the NPG core capabilities in Steps 1 & 2. They will use this as justification for HSGP funding to develop new core capabilities or strengthen others in Step 3. Many plans may be affected by new or modified core capabilities but updating the Emergency Operations Plan (EOP) in Step 4 is crucial to ensuring proper employment by Emergency Operations Centers (EOCs) during disaster response and recovery. The Homeland Security Exercise and Evaluation Program (HSEEP) offers a standard and systematic approach for validating core capabilities in Step 5. Evaluation results inform THIRA/SPR updates which, in turn, drive the next cycle of the National Preparedness System.

NPS Step	THIRA/SPR Application
1. Identify & Assess Risk	identify threats and hazards of concern and describe their impacts.
2. Estimate Capability Requirements	Develop capability targets, assess current capabilities, & identify gaps.
3. Build & Sustain Capabilities	Prioritize investments in areas that address identified capability gaps.
4. Plan to Deliver Capabilities	Develop and update plans based on capability targets and gaps.
5. Validate Capabilities	Use capability targets when assessing performance in incidents & exercises.
6. Review & Update Plans	Use evaluation results to drive continuous improvement & update THIRA/SPR.

Table 4: National Preparedness System, 2018 CPG-201

Within the context of the National Preparedness Goal and in light of the resurgent threats to US domestic territory, a number of major exercises have been conducted to test the nation's preparedness for a Black Sky Event.

- GridEx. Since 2011, the North American Electric Reliability Corporation (NERC) has sponsored the largest grid security exercise in North America. Every two years, NERC and participating agencies from the Electricity Information Sharing and Analysis Center (E-ISAC) practice how they would respond to and recover from coordinated cyber and physical security threats and incidents. [67]
- Exercise Dark Sky. In May 2018, Wisconsin held Dark Sky, a full-scale exercise simulating a long-term, mass power outage across 45 counties—approximately two-thirds of the state—affecting 2.8 million

people. The purpose of the exercise was to test existing emergency and contingency plans, and increase understanding of the coordination, policies, and procedures required to conduct a joint inter-agency response to cyber and physical threats and subsequent attacks on infrastructure. Wisconsin Emergency Management (WEM) conducted the exercise together with local emergency management officials, the Wisconsin National Guard, First Responders, and private utility representatives.

- Cascadia Rising. Cascadia Rising 2016 was a two-year effort to test and validate plans for a 9.0 magnitude earthquake along the 700-mile Cascadia Subduction Zone (CSZ) fault with subsequent tsunamis and aftershocks, impacting California, Oregon, Washington, and Idaho. The exercise spanned local, state, tribal, and federal governments, the military, private sector, and nongovernmental organizations (NGOs) in a simulated field response to the aftermath of a disastrous CSZ earthquake and tsunami. Specifically, the exercise aimed to test the ability of Emergency Operation Centers in the region to coordinate and communicate priorities and objectives, share situational information, and request, order, and transport life-saving resources to impacted areas in the event of such a scenario.
- Liberty Eclipse. In November 2018, the Department of Energy (DOE) sponsored Liberty Eclipse testing the grid's ability to bounce back from a blackout, simulating the painstaking process of re-energizing the power grid while squaring off against a simultaneous cyberattack on electric, oil and natural gas infrastructure. The goal of Liberty Eclipse was to prepare for cyber-attack on the electric grid. The exercise emphasized the black-start process for restoring electricity following a massive blackout. It also examined the Electricity Subsector's reliance on natural gas. Liberty Eclipse featured a two-day tabletop exercise for grid and oil and natural gas representatives, ahead of an operational drill of the black-start process for restoring electricity following massive blackouts. [68]

Additionally, FEMA also manages a two-year cycle of National Level Exercises under the National Exercise Program (NEP). A key component of the National Preparedness System, the NEP is congressionally mandated under Title 6, Chapter 2, Section 748 USC to "test and evaluate the capability of Federal, State, Local and Tribal governments to detect, disrupt and prevent threatened or actual catastrophic acts of terrorism, especially those involving weapons of mass destruction," and "to test and evaluate the readiness of Federal, State, local, and tribal governments to respond and recover in a coordinated and unified manner to catastrophic incidents." [69]

9/11 was a turning point for the nation and FEMA. Incorporated into the new Department of Homeland Security in 2002, FEMA started using the Homeland Security Grant Program to help forge greater interoperability and closer collaboration among the nation's Emergency Managers and First Responders. FEMA had to become better at Emergency Preparedness because the number of disasters costing over a billion dollars has increased from an average of 3/year in the 1980s to 13/year in the 2010s. [70] It is a fair assessment to say that due to FEMA's efforts the nation today is much better prepared to withstand disaster than it was before 9/11. So what more needs to be done for Civil Defense?

CD Programs & Objectives

In 1954, the United States Federal Civil Defense Agency instituted an exercise called Operation Alert, abbreviated "OPAL". It was a civil defense drill that took place on the same day in scores of major cities. Citizens in what were called the "target" areas were required to take cover for fifteen minutes. At

the same time civil defense officials tested their readiness and their communications systems, and federal officials practiced evacuating from the capital. Even President Eisenhower left the White House for a tent city outside Washington. The following day newspapers routinely published reports of the fictitious attacks naming the number of bombs that were dropped in the mock alerts, the number of cities hit, and the number of casualties. [71]

In 1955, New York State made the failure to take cover during an Operation Alert exercise punishable with a fine of up to $500 and a year in jail. A small group of pacifists that included Catholic Worker Dorothy Day reacted to this law by staging a protest in Manhattan's City Hall Park. When the air raid sirens sounded, on June 15, 1955, the 27 protesters sat on park benches, surrounded by reporters. They explained that they were protesting the government's pretense that citizens could be protected in the event of a full-scale nuclear attack. The protesters were arrested and given suspended sentences. [71]

The last of the OPAL Civil Defense exercise series, indeed the last nationwide public Civil Defense drill in the United States and possibly any NATO nation, was held in April 1961. Instead of having the public scramble for shelter, henceforth exercise resources would be put into Continuity of Government planning. This was coordinated at the Federal level by the newly restructured Office of Civil Defense (OCD) in the Pentagon and Office of Emergency Planning (OEP) in the executive branch, leading toward exercises involving key civil service employees, officials of Federal agencies and departments, and the White House. [72]

Though all fifty states and more than 2,500 county and city governments had developed survival plans, few were operational. There was no attention to post-attack resource management in the plans, even though state and local governments were responsible for provisions (including food) following an attack. As of February 1961, only thirty-eight states and just a few counties or cities with populations under 50,000 had legislated lines of succession. Duplicating and storing essential records was all very well, but they had to be maintained and kept current; no state operated a fully adequate program. All states and many large cities had alternate sites for emergency governments, but virtually none were in blast-proof or even fallout protected facilities. Few government employees at any level were trained beyond what they had experienced in OPALs, which confined exercises to just a few days following nuclear attack and never rehearsed the reconstruction or emergence from shelter phases of a post-attack world. Without improved readiness at all levels of government, the effective operation of the executive branch's ''High Point'' location at Mt. Weather, Virginia (also referred to as ''the Hole''), which had been on continuous activation since September 1958, would be fruitless. As one Civil Defense official observed, "plans are worthless if governments do not survive to execute them.'' [72]

The ''Basic Report of Civil and Defense Mobilization,'' issued in February 1961 to apprise President Kennedy of the defense situation, points out that with the development of Soviet missile systems the United States not only became more susceptible to surprise attack but active defense became increasingly vulnerable. Passive measures—population and resource dispersion and mobility, hardening of facilities, and concealment—were what remained. [72]

A 1957 study of metropolitan St. Louis, Missouri, predicted that with a minimum of fifteen minutes warning, 45–60 percent of the population could survive a large thermonuclear blast if they had access to shelters with at least 30 psi blast protection. The emerging thought was that a national system of fallout shelters, coupled with tactical evacuation in an attack on fifty cities, could save twenty million lives if there were thirty to sixty minutes' warning, or sixty million lives with between three and six hours' warning. In an attack on 150 cities, the same strategy could save seventy-five million lives with a

brief warning, or one hundred million lives with the longer period of warning. Implementation hinged on cost. [72]

A 1965 study of Houston, Texas, showed that for $201 million, 100 psi blast protection could be provided in public shelters, saving 70 percent of people in surrounding counties from a 10 megaton bomb; fallout protection alone would cost $104 million, for a 63 percent survival rate. The cost of blast protection for the general public was considered prohibitive in the United States; home fallout shelters, which put the cost onto private citizens, were favorable as far as government expenditure was concerned. [72]

To encourage planning for fallout shelters in new buildings, the Eisenhower administration's 1958 National Shelter Policy included provision for design and construction of prototype shelters in various climates and geographical areas. Some shelter proposals were far-fetched: one proposed blasting shelters out of the rock eight hundred feet below the surface of Manhattan Island, at cost of $28 billion. Other proposals for different degrees of fallout or blast protection for urban as well as rural populations ranged up to $115 billion for the entire nation. Proposals that also provided blast protection averaging 100 psi brought the cost up to $528 per person. Achieving this would occupy the entire construction industry for years. There was hesitation over exactly what to do despite consensus that shelters could protect against fallout. The federal government favored, not surprisingly, surveying potential existing public shelter in target areas (estimating costs for this at just $13.6 million) and encouraging homeowners to install their own shelters, using Federal Civil Defense Agency designs for which training and education would cost the government merely $1 million. [72]

The logistics of protecting the public in an attack focused Civil Defense efforts, but at the same time the problem of securing public cooperation also preoccupied planners. This was approached primarily through education and advertising campaigns coordinated through the mass media. In the US, Civil Defense curricula were promoted in grade schools as well as adult education programs. The hope was these efforts would result in behaviors compliant with Civil Defense planning. Americans who attended public school during the administrations of every president from Harry Truman to John F. Kennedy remember how to ''duck and cover.'' In August 1950, just after the outbreak of the Korean War, school civil defense drills began in major American cities. By late 1952, civil defense training was present in 87.4 percent of elementary schools and 88.4 percent of secondary public schools. From 1952, the drill procedure—every two weeks in many places — was promoted to grade school students by a comic book featuring a prudent turtle, Bert, who took cover in his shell whenever he saw ''the flash.'' In January 1952, Bert was immortalized in an animated film. Schoolchildren were supposed to follow Bert's example: drop to their knees, either hunch over as tightly as possible or lie flat facing the ground, and clasp their hands behind their necks. These postures were intended to make a human being a smaller target for projectiles, avoid retinal burns, protect the abdominal organs, and prevent the neck vertebrae from being severed. To duck and cover under one's desk gave added security. [72]

Despite enduring skepticism among the public, the summer of 1961 was the height of the fallout shelter craze, sparked in part by President Kennedy's speech recommending personal shelters and huge appropriations for government spending on Civil Defense. The president's letter to the people in a September 1961 issue of Life magazine, printed over a picture of a mushroom cloud, emphasized the importance of the shelter survey program and his recommendation to Congress that the public shelters be stocked. President Kennedy's May 1961 speech set off a frenzy of interest in prefab home shelters. The Peace-O-Mind Shelter Company in Stephenville, Texas, Atlas Bomb Shelter Company in Sacramento, and Chicago's Wonder Building Company were just a few manufacturers. However, the happy portraits

of close-knit families did not persuade many Americans to build or equip home shelters. Americans were curious, but seldom matched curiosity with expenditure. Even President Eisenhower explained that he would not build a shelter on his Gettysburg, Maryland, farm out of concern that this would alarm his neighbors. A scandal erupted in New York state when the speaker of the state assembly, who had railroaded through legislation on shelters, turned out to be director of a company that made them. Concerns were rife about shelter scams, hucksters who sold prefabs that offered little radiation protection, and fly-by-night companies that did not fulfill contracts to install shelters. A Life cover story in January 1962 raised more skeptical questions about the shelter movement. It included comments by people from many walks of life expressing pro, con, and ambivalent viewpoints. The American public was extensively surveyed on their opinions about the likelihood of nuclear war, their perception of local risks, knowledge of Civil Defense principles, and inclination toward participating. Despite the efforts of the government and the enormous publicity accorded to civil defense, few Americans built shelters, and even fewer considered moving to reduce their risk. [72]

In contrast to generally widespread public participation and acceptance in the peak years of Civil Defense during the early stages of the Cold War, most people only a decade later in the 1970s had little faith that any government Civil Defense planning could lessen the impact of nuclear war. Some local communities refused outright to cooperate with Federal Civil Defense mandates because they did not believe they would be effective if a nuclear attack were to occur. This public attitude would continue throughout the remainder of the Cold War period. [58]

National Plan for Emergency Preparedness

The 1964 National Plan for Emergency Preparedness (NPEP), drafted under the Kennedy Administration shortly after the Cuban Missile Crisis, provides historical insight into US Civil Defense policy at the height of the Cold War. According to the NPEP, US Civil Defense Policy was guided by two overarching policies:

1. Survival and Recovery.
2. Preservation of Rights and Values. [15]

In the period immediately following attack upon the United States, national survival and recovery would be the primary objective. In order to achieve this, efforts were to be directed to defense and retaliatory operations, to the saving of life and property, and to essential aid to allied nations. The government of each State was responsible for the preparedness and emergency operations of the State and its political subdivisions and for insuring that such activities were compatible with those of the Federal Government. The government of each political subdivision was responsible for its preparedness and emergency operations in accordance with Federal and State emergency plans and programs. While the Federal Government could indicate the kinds of preparedness actions the States should take, it was the responsibility of the State governments to provide the additional constitutional or statutory support, organization, and procedures for the conduct of those activities. The same was true of the need for local ordinances to meet the preparedness requirements of each county and municipal locality. [15]

Although the Government would take whatever action was required to ensure national survival in times of great peril, it did not mean the end of personal and political freedoms. One of the fundamental policies of the emergency preparedness program was that measures in response to emergency conditions should be taken without undue infringement of individual rights and with minimum disruption of the political, economic, and social structure of the Nation. this meant that

Martial Law would only be imposed in extreme situations when civil government was unable to act. However, if neither a State nor Local government could provide emergency services, the Federal Government should assume responsibility to the extent necessary and possible. [15]

EP vs. CD

Despite having disappeared since the Cold War ended thirty years ago, it would appear that Civil Defense and Emergency Preparedness share many commonalities.

NPEP	NPG	Commonality
X	X	1. Objective to protect domestic population from disaster.
X	X	2. Objective to rapidly recover from disaster.
X	X	3. Objective to maintain constitutional law and protections.
X	X	4. Objective to maintain Continuity of Government.
X	X	5. Preparedness and response authorities with Federal, State, & Local governments.
X	X	6. Central Federal agency has legal authority to advise and coordinate Civil Defense matters.
X	X	7. Central Federal agency facilitates disaster planning with Federal, State, & Local governments.
X	X	8. Central Federal agency facilitates disaster exercises with Federal, State, & Local governments.
X	X	9. Defense Support of Civil Authorities
X	X	10. Individual self-reliance and sufficiency until basic services can be restored.

Table 5: CD vs. EP Commonalities.[17]

By the same token, some notable differences still remain between Cold War CD and contemporary EP.

Difference	CD	EP
1. Disaster scope.	Nationwide	Regional
2. Primary protection emphasis.	Nuclear – Fallout Shelter	All-Hazard
3. Secondary protection emphasis.	Nuclear – Urban Evacuation	All-Hazard
4. Public awareness & participation.	Formal – Grade School Curriculum	Informal – Advertising
5. Federal agency organization.	Divided – Military & Civil	Unified – FEMA

Table 6: CD vs. EP Differences.[18]

FEMA has a number of options it may consider for addressing the identified differences between Cold War CD and contemporary EP.

Difference	Options
1. Preparation for nationwide disaster.	1. Nothing
	2. Conduct CD National Level Exercises
	3. Fund HSGP Exercises That Assume No NRF Support
2. National sheltering program.	4. Nothing
	5. Advocate National Shelter Program
	6. Advocate Congressional Funding
3. National evacuation program.	7. Nothing
	8. Conduct CD National Level Exercises
4. Public education curriculum.	9. Nothing
	10. Fund Grade School Curriculum
	11. Conduct CD National Level Exercises
5. Split civil-military responsibilities.	12. Nothing
	13. Split FEMA Responsibilities with DOD

[17] Other similarities include emergency warning and broadcast; these are but some of the commonalities.
[18] Likewise, there are probably many more differences; these are some of the more prominent ones.

Table 7: Options for Addressing CD & EP Differences.

Findings

Given everything that has been examined to this point, we believe the following findings succinctly summarize a practical end state for 21st Century Civil Defense.

1. Nuclear attack, EMP, or cyber-attack, all will incapacitate critical infrastructure.
2. Rapid recovery will depend on how quickly critical infrastructure can be repaired.
3. Restoring electricity will expedite repair of critical infrastructure.
4. Continuity of Government will be essential to organizing recovery efforts.
5. State Governments should expect no support from Federal Government.
6. Federal Government should expect no support from State National Guards.
7. State Governments should prepare to deliver basic necessities until infrastructure restored.
8. Civil Defense activities need to be re-incorporated into national planning frameworks, regularly, tested, trained, and exercised specifically for wartime and state adversarial incidents with national impacts.
9. Historical limitations of Civil Defense activities now have new viable paths for implementation given technological advances.

Insights

Civil Defense has no formally agreed definition, but it is generally accepted to mean the protection of domestic civilian populations from deliberate attack. Civil Defense became a concern when Germany began bombing cities from Zeppelins in World War I. The threat of Japanese attack on the West Coast made Civil Defense a US concern during World War II, but it didn't become a significant concern until the Soviet Union acquired the atomic bomb and the means to deliver it during the Cold War. President Truman signed the 1950 Civil Defense Act creating an agency with the authority to advise and coordinate Civil Defense preparedness and response with Federal, State, and Local, Tribal, and Territorial governments. The overall Civil Defense strategy, as presented in the 1964 National Plan for Emergency Preparedness, was to survive a nuclear attack and quickly recover the nation afterwards. Sheltering and evacuation were promoted and exercises staged to test them. Despite these programs, the US population was not prepared when Kennedy confronted Khrushchev in the 1962 Cuban Missile Crisis. Although nuclear war was narrowly averted, public Civil Defense exercises ended in 1961 and public support for Civil Defense programs began to wane as did congressional funding. By the 1980s, some communities actively opposed Civil Defense saying it was immoral. The threat of World War III seemed to evaporate as did Civil Defense after the Soviet Union collapsed in December 1991. The Civil Defense Act was repealed in November 1994 and its remaining authorities amended to Title VI of the 1988 Stafford Act. Surviving CD authorities remain vested in FEMA under Title 50, Section 3042 USC. After the end of the Cold War, Civil Defense was all but replaced by Emergency Preparedness, the basic difference of which is scope. Civil Defense prepared for a nationwide disaster whereas Emergency Preparedness mainly prepares and responds to regional disasters, whether natural or manmade. Then on September 11, 2001, nineteen hijackers attacked the US and inflicted as much damage as the Imperial Japanese Navy on December 7, 1941. 9/11 was a turning point for the nation and FEMA. Incorporated into the new Department of Homeland Security in 2002, FEMA started using the Homeland Security Grant Program to help forge greater interoperability and closer collaboration among the nation's Emergency Managers and First Responders. In 2004, States applying for HSGP funding had to

comply with the National Incident Management System including the Incident Command System providing a standard means for agencies to effectively work together in a disaster. In 2008 FEMA made the National Response Framework a requirement for HSGP funding, providing a standard means for rapidly acquiring emergency resources across jurisdictions. Since 2012, States must justify HSGP funding for developing and improving 32 Core Capabilities as part of the National Preparedness Goal for building more resilient communities. The National Preparedness System is a continuous improvement program that validates NPG Core Capabilities through Federal, State, Local, Tribal, and Territorial exercises. FEMA had to become better at Emergency Preparedness because the number of disasters costing over a billion dollars has increased from an average of 3/year in the 1980s to 13/year in the 2010s. It is a fair assessment to say that due to FEMA's efforts the nation today is much better prepared to withstand disaster than it was before 9/11. So what more needs to be done for Civil Defense? Fallout shelters are no more available today than they were during the Cold War, and probably less so. Only public support and Congress can fix that. Urban evacuation is a lesser substitute, but it remains to the States to decide upon strategy. Both options are questionable in the event of EMP or cyber-attack. Rapid recovery, otherwise known as resilience, is best under all circumstances. FEMA already advocates and supports resilience through the NPG and NPS. However, the National Disaster Recovery Framework, and electricity, nuke, and cyber incident annexes are all predicated on the ability to call on Federal resources following a disaster. Given FEMA's experience responding in rapid succession to hurricanes Harvey, Irma, and Maria in 2017, it seems unlikely that any Federal support will be available following a nationwide disaster. FEMA can use HSGP funding to address this. By the same token, the National Guard will be essential to State recovery plans. FEMA should broker discussions through USNORTHCOM to address this contingency. Finally, FEMA might consider conducting more National Level Exercises examining Continuity of Government and Black Sky Events at all levels of government. We can hope for the best, but we must plan for the worst.

Civil Defense Lessons Learned from the Ukraine War – Conventional Challenges

The Ukraine-Russia War has demonstrated a number of lessons learned from conventional challenges, civil defense, critical infrastructure protection, and humanitarian crisis response stemming from the mass exodus of millions of refugees across Europe and globally. While this report primarily focuses on high impact threats to the homeland such as the threat of full unmitigated nuclear war with Russia as a consequence of U.S. support to Ukraine, this section briefly highlights conventional wartime civil defense issues that are more likely to apply in smaller conflicts. These lessons learned are examined with an eye towards the pacific and future conflict with China that may not necessarily rise to full nuclear exchange between nations, but more likely result in rapid seizure and smaller scale territorial conflicts. These conventional challenges will likely apply to conflicts over U.S. territory in the pacific, including support and defense of Taiwan in a war with China or plausible aggression from North Korea against South Korea. We preface that war or territorial conflict in the pacific presents its own complex challenges as it pertains to civil defense and especially that of its humanitarian impacts that should be fully investigated, studied, exercised, planned, and prepared for to mitigate potential, threatened, or actual consequences.

Homeland Defense & Civil Defense Lifeline Critical Infrastructure Priorities

One of the common targets impacted in the Ukraine-Russia War has been critical infrastructure. As it is likely that the U.S. land component in today's security environment will be tasked to conduct

critical infrastructure protection (CIP), physical protection to vital infrastructure facilities insights from this war offer value to combatant commanders in undertaking these missions. Various critical infrastructure sectors have been noted to be targeted, one of the most frequent targets in Russia's campaign being the energy sector. According to a British Defence Intelligence Update Ukraine – 01 December 2022:

- Since October 2022, Russia has repeatedly attacked Ukraine's electricity distribution grid, primarily with cruise missiles.
- This is likely the first example of Russia attempting to implement the concept of a Strategic Operation for the Destruction of Critically Important Targets (SODCIT), a key component of the military doctrine it has adopted in recent years.
- Russia envisioned SODCIT as using long-range missiles to strike an enemy state's critical national infrastructure, rather than its military forces, to demoralise the population and ultimately force the state's leaders to capitulate.
- Russia's strikes continue to cause power shortages resulting in indiscriminate, widespread humanitarian suffering across Ukraine.
- However, its effectiveness as a strategy has likely been blunted because Russia has already expended a large proportion of its suitable missiles against tactical targets.
- Also, with Ukraine having successfully mobilised for nine months, material and psychological effect of the SODCIT is likely less than if it was deployed in the initial period of a war.
  (UK Defense Ministry, 2022)

Further targeting of civilian populations and critical infrastructure includes healthcare facilities, emergency services and other infrastructure. The War in Ukraine provides great insights into wartime civil defense response and operations. Healthcare facilities specifically have been used to support a variety of activities during the Ukraine War. In doing so they have also become a target for hostile forces who have deliberately targeted, bombed and destroyed many healthcare facilities across Ukraine. One notable example being "a maternity hospital that was damaged by shelling in Mariupol, Ukraine, on March 9" where pregnant mothers were wounded and had to be evacuated [73]. This is but one of many horrific incidents witnessed during the Ukraine War. It is noted that this is not an isolated event either. According to wartime reporting, "Russia's 226 attacks on health-care targets in Ukraine are part of a larger pattern" [73]. As the United States has not suffered from or been exposed to conflict on the Homefront since World War II, it is imperative that the lessons learned from the Ukraine war as they pertain to civil defense and wartime healthcare system operations be closely examined, researched, reviewed and practices, standards and wartime operating guidelines be developed to prepare healthcare systems and other critical infrastructure such as emergency services for potential future conflicts from adversarial nations.

FEMA prescribes to a Community Lifelines model that prioritizes seven critical infrastructure sectors for immediate recovery and stabilization spanning: safety and security, food, water, shelter, health and medical, energy, communications, transportation, and hazardous materials. According to FEMA, "A lifeline enables the continuous operation of critical government and business functions and is essential to human health and safety or economic security. Lifelines are the most fundamental services in the community that, when stabilized, enable all other aspects of society to function. FEMA has developed a construct for objectives-based response that prioritizes the rapid stabilization of Community Lifelines after a disaster. The integrated network of assets, services, and capabilities that provide lifeline services are used day-to-day to support the recurring needs of the community and

enable all other aspects of society to function. When disrupted, decisive intervention (e.g., rapid re-establishment or employment of contingency response solutions) is required to stabilize the incident" [74]. This model provides guidance for local and state authorities during emergency responses.

Table 8: FEMA Community Lifelines [74].

The lifeline model provides a framework that can be used to support the prioritization of communities during wartime activities with the support and protection of defense assets. However, one identified change stemming from wartime activities may necessitate changes to this model to include protection and prioritization of the defense industrial base critical infrastructure sector in support of national defense activities and sustainment expanding the approach to this model. Limited civil defense capabilities may likely necessitate even further reprioritization of these seven sectors into an even smaller more manageable critical infrastructure protection list dependent on resources during civil defense operations. The expansion reflects the unique type of incident response, likely overarching national defense priorities of the defense industrial base, vital domestic manufacturing capabilities, and the need for continued delivery of mission critical supplies, materials and systems in support of the protection and defense of U.S. sovereignty. Examples of supply chain, economic impacts and disruptions that result, can be drawn from recent a "War-Game 'Conflict' with China" tabletop exercise, where the U.S. in a potential scenario entered into conflict with China in defense of Taiwan [75]. The exercise was conducted by the Center for New American Security for U.S. lawmakers who are quoted as saying "the

most glaring shortfalls appeared in diplomacy and in nonmilitary planning" identifying the need for a reexamination and reevaluation of lifeline critical infrastructure and other critical supporting elements such as national supply chains, materials production and acquisition during wartime incidents in advance of conflicts [75]. A clear, demonstrated need for action, partnership, and planning before the next conflict. Notably, its recommended that USNORTHCOM, HDI, DHS, FEMA, and CISA can work to address this issue now for civil defense preparedness and long-term supply chain disruption mitigation, prevention, and preparedness for securing national and mission critical materials and supplies. This includes discussions and expansions on the implementation and usage of the Defense Production Act and DHS and FEMA's authority and role in its implementation.

Mass Exodus – Logistical Challenges Evacuating Major Populations from Warzones

One of the most challenging issues stemming from the Ukraine War is the massive exodus of 15 million+ population from warzones. The issue of mass evacuation is one of the major contemporary issues with civil defense that should be intensively examined. Especially in light of recent incidents in Afghanistan with the 2021 Kabul Airlift and presently with evacuations underway in Sudan. U.S. lessons learned from these incidents and from the Ukraine-Russia war provide critical insights into managing the challenges facing rapid global military logistics. Mass population evacuation should not be taken lightly, these are intensive efforts that require coordination among numerous governments, agencies, and organizations, including the private sector and non-profits who are needed to successfully support and assist in managing the execution of operations on this scale. One vital lesson learned from all three recent incidents is that no single nation is capable of handling mass evacuations on this scale alone. International partnership, coordination, communication, shared resources, and assets are critical to such efforts. Advanced planning for such mission requirements is strongly encouraged. This continues to be a reoccurring mission area for defense support with many historical precedents. Much in terms of lessons learned can be drawn from present and past conflicts and incidents. As such, it is strongly recommended that review of rapid global logistics capabilities and systems, emergency reserve sea, land, and airlift be examined as it pertains to civil defense and military support requirements towards the critical mission of mass population evacuation from both warzones and during disasters.

Emerging Tech – Generative AI for Civil Defense Planning

With the advent of major technological innovations and breakthroughs since the inception of civil defense, new means of solving civil defense challenges have risen in unexpected ways. The use of generative AI and machine learning such as Chat GPT 4.0 for civil defense planning, exercises, operational support, decision support, subject matter data retrieval, and public massaging are but a few examples of areas in which civil defense support can be revolutionized through AI integration. The possibilities are endless. Operational support and decision-making is a unique area where, it is envisioned that the traditional war room or emergency operation center model where dozens to upwards of even one hundred or more dedicated support personnel, subject matter experts, and agency representatives could be more effectively and efficiently transitioned into virtual AI driven support in times of crises. AI tools can provide new means of integrated, data driven decision support akin to cutting edge battle management software. Generative AI presents new means of solving wicked challenges in new, innovative ways. Case examples are already being seen in disaster responses internationally, and more and more potential uses continue to be identified from medical support and remote health monitoring to mental health and behavioral support, resource identification, emergency

communications support, to even alert and early warning systems for natural hazards like tsunamis. The application of generative AI and machine learning may ultimately be one of the greatest solutions and biggest impact drivers solving historical barriers and challenges to complex civil defense issues such as emergency sheltering, logistics, population protection and defense, and tipping the wicked problem and calculus underpinning strategic deterrence between two near-peer adversaries to stay in favor of the United States.

National Resilience: Commercial Space and Ukraine

It's perhaps tempting to observe the Russian invasion of Ukraine, take notes about how its forces conduct an actual invasion of another nation, and then devise a scenario in which those observations are applied to U.S. Civil Defense efforts. Yet, despite those well-meaning applications, the chance of a military invasion of the U.S. and the subjugation of its citizens by an occupying force is close to zero, if only because of the size of the occupation force required to do so successfully. [76] However, should such an ill-advised undertaking be conducted against the U.S. in the 21st century, commercial space services and technologies provide a way to increase national resilience without compromising existing civil defense programs and processes.

That resilience has been demonstrated in Russia's war against Ukraine. The invasion's results on Ukraine's citizenry parallel concerns for U.S. Civil Defense. Based on some of the reporting, Russian troops have deliberately targeted civilian infrastructure. As a result, Ukrainian citizens find themselves without power and clean water. [77] Food is difficult to come by. The medical needs of the elderly and others can't be provided for. They have limited or no communication.

The new services provided by commercial satellite operators have helped alleviate some of the inconveniences Ukrainians face. Despite Russian hacking and jamming attempts, low Earth orbiting (LEO) broadband satellites provide residents with internet access. Global Positioning System (GPS) satellites provide positioning, navigation, and timing (PNT) signals so people can find their way through areas rendered unrecognizable due to Russian shelling. The prevalence of imagery satellites may not be immediately meaningful to residents, but their updated images provide Ukraine's government with another tool to identify regions requiring aid.

However, commercial satellite operators don't create their services with the intent to limit them. By their nature and desire to dominate a market, businesses usually make onboarding new customers easier. This may mean there are few background checks on customers wishing access to these services. That, in turn, could result in using these commercial space assets in a way that their owners never intended. It is already happening with SpaceX's Starlink. [78]

Increasing National Resilience: Commercial Space Infrastructure and Services

One aspect requiring more thorough study is the newer possible challenges to homeland security and opportunities that commercial space companies offer customers. When civil defense programs initially began in the United States, the implications of space infrastructure weren't even a consideration. And when space assets such as satellites were deployed over the decades, the ones with payloads for Earth observation and navigation were initially under the control of government agencies. However, the landscape and space infrastructure has changed dramatically in the last ten years.

Those changes are demonstrated in Ukraine's defense against Russia. The Russian military has fully embraced and used a spectrum of electronic warfare (EW) tools and strategies, such as cyber-attacks and GPS and communications jamming and spoofing. [79] As the Russian military implemented its EW tools, it resulted in the opposing forces facing a loss of communications and the ability to coordinate forces; and a loss of satellite-provided navigation signals.

Ukraine's military had already faced Russian EW tactics and technology when Russia completed a land grab of the Crimean Peninsula in 2014. However, in 2022, Ukraine leveraged a sector that has significantly changed during the last decade: space companies and their growing portfolio of commercial products and services. Over 80% of the 2,000 commercial spacecraft deployed in 2022 were for communications. Over 250 commercial satellites were deployed for Earth observation (EO)/remote sensing (RS) missions that same year. In addition, over 100 satellites circle the Earth to provide navigation services to smartphone owners. That is a switch from a time not that long ago (about a decade) when nearly all of those services were for government use.

They provide:

1. Satellite Communications/Broadband services
2. Positioning, Navigation, and Timing (PNT) services
3. Earth observation/remote sensing (EO/RS) products and services

Satellites for Hire

Of the three segments, the first—satellite communications—is one commercial companies have exploited for decades. It is also a segment that the Russian military is familiar with, having technologies that can hack or jam those systems. However, in the past two to three years, the segment's offerings have changed as companies such as OneWeb and SpaceX deploy broadband satellites in low Earth orbit (LEO).

In 2012, ~32 communications satellites were deployed, primarily to geosynchronous orbit. [80] At the end of 2022, nearly 2,000 communications satellites were deployed, the majority into LEO. [81] More significant to the commercial industry are the consumer antennas a few of the new companies offer. In one example, consumers connect to a LEO broadband constellation using low-cost ($500), small (less than 2 ft wide), and auto-tracking phased array antennas. [82] A customer sets the antenna with a view of the sky, and it will find, track, and connect with satellites in view. The customer needs no knowledge of antenna power budgets, orbital mechanics, latitude and longitude, or whether the antenna is correctly pointed. It just works.

Satellites with EO/RS payloads have also increased during the last decade. Like commercial satellite communications services, EO/RS products and services have been available commercially for a few decades. However, their deployments were relatively small in 2012 (also ~32) compared with 2022 (~270). [80] The increased availability of spacecraft in orbit gives EO/RS consumers near-real-time updated views of areas of the Earth. In some cases, the imagery products available in 2023 are inexpensive ($20 for an image with a resolution of less than 1 meter). [83]

In 2023, commercial EO/RS satellite operators also provide more products than the traditional overhead-collected optical imagery from the past few decades. The commercial sector began offering products and services using payloads once operated ONLY by military and government agencies. For

example, there are nearly 50 commercial satellites with radar payloads in orbit and nearly 15 satellites with infrared payloads. [81] In addition, several companies operate satellites with radiofrequency (RF) detection payloads. The payloads seek out radio signals from the Earth, where the signals aren't expected to be found.

While their numbers haven't exceeded the government and military-operated PNT constellations, commercial alternatives are beginning to become available. They plan to provide significantly increased accuracy in positioning data. The companies will do so by operating more satellites than those operated by GPS in a LEO orbit.

As these space companies deploy their satellites, they outpace their military and government counterparts. For example, in 2022, commercial space companies deployed thousands of satellites into the Earth's orbit, while all the world's militaries deployed less than 100. [84] While some might argue that the quality and expense of military satellites trump quantity, it may be advisable for them to remember that "quantity has a quality of its own." Especially considering Ukraine's results as it responds to the Russian invasion of its homeland.

Offensive Communications

On the day of the Russian offensive into Ukraine, February 24, 2022, hackers attacked and disrupted Ukraine's satellite broadband internet. However, they didn't accomplish the disruption using radiofrequency methods such as jamming. Instead, they used software.

Using new malware called "AcidRain," the hackers successfully targeted and wiped "tens of thousands" of Viasat KA-SAT modems/routers offered by a third-party provider in Ukraine. [85] The attack cut off satellite network access to Ukraine's military, government, and citizens. While the attack certainly inconvenienced the nation's citizens, it slowed the Ukrainian military and government response to Russia's incursion, as reported by Reuters:

"Pablo Breuer, a former technologist for U.S. special operations command, or SOCOM, said knocking out satellite internet connectivity could handicap Ukraine's ability to combat Russian forces.

"Traditional land-based radios only reach so far. If you're using modern smart systems, smart weapons, trying to do combined arms maneuvers, then you must rely on these satellites," said Breuer." [86]

Based on Breuer's observations, the cyber-attack result—Ukraine with no satellite broadband access—wasn't surprising, considering Russia's goals for its invasion. The result should have provided the Russian military with a battlefield advantage, especially since it operated about 172 satellites during the attack's start. [87] On the other hand, Ukraine's military operated no space assets and suffered between the cyber-attack and communications jamming. The Times of Israel quoted a few Ukrainian officials:

"They are jamming everything their systems can reach," said an official of Aerorozvidka, a reconnaissance team of Ukrainian unmanned aerial vehicle tinkerers, who spoke on the condition of anonymity because of safety concerns. "We can't say they dominate, but they hinder us greatly."

A Ukrainian intelligence official called the Russian threat "pretty severe" when it comes to disrupting reconnaissance efforts and commanders' communications with troops. Russian jamming of GPS receivers on drones that Ukraine uses to locate the enemy and direct artillery fire is particularly intense "on the line of contact," he said. [88]

The Russian military's initial jamming efforts, including mobile radio jamming systems, were successful. [89] In addition, it impacted the Ukrainian military's communications and networks, cutting off the nation from the world. [90] However, four days after Russian troops crossed Ukraine's border, SpaceX's Starlink terminals arrived in Ukraine, and the low Earth orbiting (LEO) broadband service was turned on for the region.

Low-hanging Commercial Satellite Communications and An App For Destruction

The task of jamming thousands of LEO Starlink satellites and deploying tens of thousands of small, low-profile phased array antenna terminals proved too much for Russian jamming capability. SpaceX also adapted its antenna terminals' software in anticipation and occasionally as a reaction to Russian hacking efforts. [91]' [90] As a result, Ukraine's citizens could get internet access, and its government and military could coordinate operations countering the Russian incursion.

That coordination using space assets was a hard lesson Ukraine's military learned during Russia's invasion of Crimea in 2014. In that invasion, the Russian military sabotaged the Russian-made radio handsets used by the Ukrainian military. It also used its communications jamming to isolate Ukrainian units and geolocate their position. [92] When that was accomplished, Russian artillery would hammer the uncoordinated Ukrainians with artillery and rockets. [89] However, in 2022, Ukraine's troops used Starlink and a smartphone app to turn the tables on this Russian tactic.

Geographic Information System of Artillery (GIS Arta) is a software application developed for the Ukrainian military. It can be installed on computers, tablets, and smartphones and appears network agnostic. The application allows Ukrainian forward observers, unmanned aerial vehicles, and others to share a target's location in real-time. Others can verify the target, then request fire (artillery, rockets, ambush) from available elements. It all can be accomplished in about a minute. [93]

The Starlink satellites and antenna terminals provided the network for Ukrainian troops to effectively use GIS Arta, directing attacks against Russian troops within minutes of observing them. It also allowed for the command and control of unmanned aerial vehicles to observe Russian troop movements and bomb tank columns. In addition, the network connection was a boon for Ukraine's government, allowing Ukraine's prime minister to speak to Ukrainians and the world. Moreover, it allowed the Ukrainian government to dispute Russia's Vladimir Putin narratives with graphic images of carnage on the battlefield, usually at the expense of the Russian military.

The Russian jamming of Ukrainian communications halted, however, primarily because the jamming impacted Russian communications negatively. The Russian military had no equivalent to Starlink that it could rely upon. In June 2022, a U.S. general noted:

"What we're learning now is that the Russians eventually turned it off because it was interfering with their own communications so much," said retired Lt. Gen. Ben Hodges, a former US Army commander for Europe." [88]

The satellite broadband disruption might have been worse between the jamming being halted, SpaceX stepping in with its Starlink terminals and service, and other nations coming to Ukraine's aid. [94] But, simultaneously, the cyber-attacks and communications jamming supporting the Russian invasion were expected. The cyber-attack spillover, however, might not have been—at least, not from communications companies' customers.

Collateral Damage: Communications

"If you target a satellite that is providing certain services to a specific country involved in a conflict, you might also be depriving a neutral country of the services that same satellite provides, therefore breaching that rule of neutrality," Ortega says. "The reverberating effects of attacking these infrastructures can have effects that would be very deeply felt by civilians." [95]

On the same day, February 24, 2022, German wind turbine operators saw their remote monitoring and control systems fail for nearly 6,000 wind turbines. The result?

"Due to a massive disruption of the satellite link in Europe, remote monitoring and control of thousands of Enercon wind energy converters (WECs) is currently only possible to a limited extent," German wind turbine manufacturer Enercon said today. [96]

The combined power output of those turbines equaled 11 gigaWatts. The turbine operators also relied on a third-party operator's modems for their satellite communications with Viasat's KA-SAT satellite (an estimated 30,000 European satellite modems were impacted). [96] Germany activated its national IT crisis response center to respond to the problem. [97] Other European nations, such as Poland, the Czech Republic, and Slovakia, also experienced satellite communications outages due to the cyber-attack. [86] As with the attack on Germany's turbines, in the cases of those nations, it's not clear that hackers deliberately targeted their modems. However, even if the disruptions were accidental, the consequences continued for longer than a month after the cyber-attack. [95] In addition, unlike Ukraine, cyber-attack victims in other nations using Viasat's satellite were not given an alternative communications link. Instead, they had to rely on Viasat and the third-party company to replace their modems, a tedious and lengthy process considering the thousands of compromised modems—far longer than the four-day communications outage Ukraine experienced.

By targeting the modems of a specific satellite, in this case, Viasat's KA-SAT, the cyber-attack was theoretically very specific in the impacted equipment. Despite targeting a particular satellite modem, its provision to customers beyond those in Ukraine meant they would (and did) also feel the cyber-attack impacts. It seems to have exploited a tendency of the third-party satellite operator that is common among many companies: irregular security updates/patches. [98] That exploit remained open despite warnings from U.S. and UK cybersecurity organizations, but perhaps only some people paid attention to those warnings. For example, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) warned about the increasing possibility of cyber-attacks due to the upcoming Ukraine-Russia conflict. [99] Viasat may have received that warning. However, it's unclear if the company passed it along to the third-party vendors providing modems to customers using Viasat's satellite. It may also be that vendors ignored CISA's and others' warnings. Despite individual and collective efforts to identify who was behind the attack, no specific attacker has been officially identified. However, U.S. intelligence analysts believe Russian hackers were the most likely culprits. [100]

Complementing U.S. Civil Defense Communications

Using Starlink for this example because it's the only system of its kind operational in 2023 (OneWeb uses different terminals). The Starlink satellite terminals' low cost and simple setup, coupled with the ubiquity of an orbiting satellite network connection, may augment existing U.S. Civil Defense-oriented emergency communications systems. In addition, using it could help quickly establish a comprehensive and accessible broadband network in impacted areas with minimal infrastructure

requirements. Additionally, the expertise necessary for establishing a network connection is low, on par with the knowledge required for connecting a broadband modem. Ukraine required four days to regain internet access because no pre-existing agreement existed between the government and SpaceX to provide Starlink. That agreement and the shipment of terminals from the U.S. to Ukraine delayed the country's access to communications.

Global Positioning System Jamming

That the Russian military used GPS jammers before and during its invasion of Ukraine shouldn't be surprising. [101] As with its communications jamming and hacking, throughout the years leading up to February 2022, the Russian military developed and used more sophisticated GPS jamming systems. [102] Also, GPS spoofing techniques protect Russian leadership within Moscow and while traveling, which can have some interesting side effects. [103] However, a few analysts have noted that the Russian military's jamming of GPS signals during the campaign has not been as aggressive as anticipated. One guess why GPS signals still make it to Ukraine's ground forces is that Russian troops also rely on GPS. From an interview with Professor Serge Besanger, Professor, ESCE International Business School:

"In fact, GPS receivers are very popular, much cheaper and easier to use than Glonass receivers. As evidence, downed Russian fighters were found to have civilian GPS receivers attached to their dashboards. Their system, Glonass, depends on terminals produced in very small quantities so there is no effect of scale; GPS terminals are produced everywhere and cost 10 euros, so it is cheaper for a Russian aviator, for example, to get a GPS terminal in China and fix it to the dashboard than to wait for his superiors to find him a Glonass terminal." [104]

GLONASS is the Russian counterpart to the United States GPS.

For the Russian GPS jamming facing the Ukrainian military, the Ukrainians devised an obvious solution against the jamming: use a different space-based navigation system. There are at least six space-based positioning, navigation, and timing constellations orbiting the Earth: GPS (USA), GLONASS (Russia), BeiDou (China), NavIC (India), Galileo (Europe), and QZSS (Japan). Ukraine's drones can switch to using BeiDou. China's PNT constellation is fully functional for global use. It also uses a different frequency than the GPS constellation and circumvents Russian PNT jamming efforts. [105]

Demonstrating GPS' inadvertent utility, even when those who intimately understand it forget its ubiquitousness: while the Russian military has shown proficiency in jamming GPS signals, it missed a critical hole in its information security for its troop movements.

As Russian troops made their way to Ukraine's border hours before the invasion, Google Maps, a common smartphone application that uses GPS, marked highly unusual congestion of the routes they took in red and orange. For example, the one between Russia's Belgorod and the Ukrainian border was 40 kilometers long, all caused by Russian troop movement to the border. [106] Once discovered, Google turned off the traffic update feature.

Collateral Damage: Positioning, Navigation, and Timing (PNT)

Despite the Russian military's proficiency with GPS jamming systems, civilian commercial airlines succumbed to the tactic. [107] Airlines with routes near eastern Finland, Turkey, Cyprus, Syria, the Black Sea, and Kaliningrad had aircraft that experienced GPS navigation disruption from nearby Russian GPS jammers. [108] The European consensus is that the disruption of space-based navigation signals from

sources inside Russia is inadvertent. However, the disruption is still causing the Europeans to react to avoid mishaps caused by the jamming.

The disruption was enough to cause the European Union Aviation Safety Agency (EASA) to release a bulletin in mid-March warning of intensified GPS spoofing and jamming. [109] In addition, there were some instances in which airlines could not complete the short flight between Finland's Helsinki (near the southern tip of the country) and Savonlinna, in eastern Finland. [110] Another example: in December 2022, citizens of cities and areas inside Russia were dealing with GPS signal interference. [111] Combined with the anecdotes of Russian pilots taping GPS terminals into a fighter cockpit, this scenario confirms a viable lack of a PNT alternative for Russians. The Russian military's GLONASS satellites orbit the Earth, but the dearth of GLONASS ground terminals that can receive those signals demonstrates the system's irrelevance to Russia's citizens. So instead, Russian citizens are relying on chipsets in their devices, which typically use GPS signals for navigation and other purposes.

However, Russia is also using GPS and another space-based technology to its advantage differently: it's disguising maritime tracking transponders on Russian ships to evade sanctions. [112] The Automatic Identification System (AIS) tracks ships to minimize a ship's collision risk and avoid delays. It's mandatory for ships above a specific tonnage; part of its transmission contains GPS location data—several hundred satellites orbiting the Earth aid in tracking ships with AIS.

However, particular Russian (and North Korean) ships allow for the AIS to be shut off and can change the ship's identifier associated with a particular AIS. Evidence of this tampering occurred in December 2022, as a Russian-flagged ship left port in Istanbul but never arrived in port at Novorossiysk, Russia. [113]

Complementing U.S. Civil Defense Location Efforts: Leveraging the Numbers

The advent of the smartphone with GPS chipsets has simplified this process for U.S. Civil Defense purposes. That device can help a person identify their location. However, a smartphone with a network connection allows that person to contact authorities and pass on location information to receive aid and report conditions.

The pervasiveness of smartphones to U.S. consumers indicates that little investment is required to help them from a U.S. Civil Defense perspective. It also points to exploring options for leveraging the presence of the technology to augment search and rescue efforts and other activities.

Commercial Earth Observation (EO)/Remote Sensing (RS) Products and Services

Unlike space-based communications and PNT technologies, Earth observation/remote sensing appears not to have endured collateral damage during the Russian invasion of Ukraine. Commercial imagery from satellites has increased during the Russia/Ukraine conflict. Despite Russia's advantage over Ukraine in the number of satellites it operates, Ukraine has leveraged satellite images from commercial companies. U.S. companies such as Blacksky, Planet, and Maxar have provided imagery covering impacted areas in Ukraine.

Unlike its reaction to LEO broadband operators, where the Russian military threatened to attack their satellites, it seems to have ignored the commercial EO/RS satellite operators. [114] It may be that the hundreds of commercial EO/RS satellites orbiting the Earth may have caused Russian military leaders to believe that physically attacking them would be futile due to the redundancy. On the other hand, it

may be as simple as the Russian military doesn't consider the imagery to be imparting vitally important information. The Ukrainian government, however, has used satellite imagery to help its cause.

Evidence of Ukraine's use of satellite imagery appears in weekly—sometimes daily—releases of news stories. These stories contain the most recent overhead images of the battlefield, destruction of communities, evidence of gravesites to hide war crimes, and more. Satellite images of villages and cities taken before the invasion are compared with images of them after shelling by Russian troops. [115] Imagery from Russian Earth observation satellites has been non-existent during Russia's attempt at conquering Ukraine.

The nation has the space assets to provide imagery. Still, if it has released satellite images, they have yet to gain the traction the commercial imagery providers have maintained for their Ukraine-supporting imagery. However, releasing those images to the public may prove self-defeating to the Russian leadership and its evolving attempts at weaving a self-defense justification for its invasion.

The commercial images Ukraine releases to the public have vividly and concretely refuted Russian narratives of self-defense and progress in the war. The constant releases of those images remind observers around the world of war's realities, which in turn may increase sympathy towards Ukraine while feeding an antipathy towards Russia's interests.

Satellites that can track radio jammers against communications and GPS satellites are also beginning to be commercially run. For example, Hawkeye360's radiofrequency detection satellites detected, identified, and located GPS jammers near or within Ukraine in the days leading up to the invasion in February 2022. [101] However, the company noted in the same press release that GPS jamming equipment is readily available, inexpensive, and easy to deploy.

Complementing U.S. Civil Defense Situational Awareness

The growth and accessibility of commercially provided satellite imagery may be used to augment efforts to determine how an area has been impacted. U.S. Civil Defense efforts would require no purchasing and operating of satellites to gain access to these products. It would not need to build and operate a ground system to operate those satellites.

Commercial satellite images tend to be less detailed than available images from government-run imagery satellites. However, there may be delays in gaining time-sensitive imagery for responding to a situation because there are fewer government imagery satellites. On the other hand, commercial imagery satellite operators can provide "good-enough" satellite imagery relatively quickly. For example, the hundreds of orbiting commercial imagery satellites guarantee the ability to purchase and view near-real-time imagery. Authorities could determine the extent of an event's impact by comparing an area's before and after images.

Growing Competition=More Opportunities for Increasing National Resilience?

The changes and growth the commercial space sector is undergoing are mainly due to the competitiveness among newer space startups. The examples provided for the different markets—communications, PNT, and Earth observation—are the latest successful instances of products and services. Other startups are deploying, or planning to deploy, even more satellites to cater to those markets, some with a different take on what customers may want.

For example, in the LEO broadband market, Amazon is about to deploy two pathfinder satellites of a planned constellation of over 3,000 satellites. [116] In addition, some startups have or are beginning to deploy commercial alternatives to government and military-run PNT systems, such as GPS and GLONASS. For example, Xona Space Systems already has two pathfinder satellites in orbit and plans to deploy nearly 300 satellites for commercial PNT services. [117] However, most competition is in the commercial space-based EO/RS market.

The most well-known EO/RS startup, Planet (formerly Planet Labs), operates ~250 satellites in LEO. The company's satellites can capture optical imagery with a resolution of fewer than 12 inches (30 cm). [118] The large number of satellites the company operates lets it collect information about any specific site on the Earth's surface about every 30 minutes. However, other EO/RS companies are deploying or planning to deploy hundreds of satellites, some for optical imagery missions, others that will use radar and infrared sensors, and radiofrequency receivers.

Many of these satellite operators are U.S. companies and determining the extent of their offerings could contribute significantly to more resilience for a Homeland Security/Defense response. Other than contracts for services and products, there is no requirement to invest in major national infrastructure projects, no need to train system operators, and no budget necessary for infrastructure maintenance. However, each competitor in the space industry brings the potential to increase national resilience.

Bringing It Together

Satellites and the products and services they help generate are not the ultimate solutions to Homeland Security/Defense, whether operated by the government or commercial companies. For example, they do not provide clean water nor defend against radiation from fallout. However, they can provide many assets to help respond to several scenarios concerning both. Additionally, the growth of commercial satellite operators provides more resiliency at a national level while requiring little in the way of spending and people. Tying them together and leveraging what they bring, using their strengths to respond quickly and intelligently, as the Ukrainians appear to be doing, could help the U.S. resolutely bounce back against an invasion of the homeland.

Part 4: How Can USNORTHCOM Support Civil Defense?

FEMA has gotten quite proficient at helping State and Local governments prepare and respond to natural disaster. The problem is even the largest natural disasters are only regional. Large parts of the nation remain unaffected and provide a safe haven from where disaster assistance can be deployed. This would not be the case following a nationwide nuclear, EMP, or even Cyber attack. There would be no safe havens from where to mount assistance. FEMA would be overwhelmed. The National Response Framework would likely fail. States would be on their own. State Governors would need every resource at their disposal to restore basic services and deliver food, water, and medicine. They would likely hold on to their National Guard. They would likely ask for assistance from local military installations.

Military installations have manpower, supplies, and transportation that would prove most helpful to State Governors following a nationwide attack. DOD Directive 3025.18 gives local commanders immediate response authority to save lives and prevent suffering. However, in the wake of a nationwide attack, local commanders might be understandably reluctant to share their resources. In the wake of a nationwide attack, Defense Support of Civil Authorities might be the key to resilience that

the 2022 National Defense Strategy says is essential to Homeland Defense. But how will USNORTHCOM perform DSCA when FEMA is overwhelmed and the nation is in shambles? Perhaps they can adapt and improvise as they did following Hurricane Maria in 2017. Or perhaps better, they can plan ahead and have authorities and procedures in-place so local installation commanders don't have to wait on orders when the State Governors come asking for assistance.

Recommendations

The absence of permanently assigned forces and Posse Comitatus present challenges to developing DSCA contingency plans, but nothing that can't be overcome. Or perhaps such plans already exist, but when was the last time they were updated? And equally important, when was the last time they were exercised with FEMA? Although FEMA created the National Disaster Recovery Framework, exercises still tend to focus on regional disasters, not ones that are nationwide. USNORTHCOM might want to broker discussions with FEMA promoting exercises that examine what happens when the National Response Framework fails. USNORTHCOM might also want to participate and use this opportunity to gain insight to State and Local requirements to help develop or update DSCA contingency plans.

What about fallout shelters? They were deemed the most effective means of protecting the domestic population from nuclear attack. It seems a national program to build fallout shelters would receive no more public support today than it did during the Cold War, perhaps even less. What about improved anti-ballistic missile defenses? USNORTHCOM already has operational control over 44 missiles deployed to Vandenberg Air Force Base and Fort Greeley. Unfortunately, they are insufficient to counter a mass strike by Russia or China, and perhaps even North Korea. For understandable cost reasons the current system is a shadow of the one envisioned by the Strategic Defense Initiative. Perhaps forty years of technological advances, particularly in reusable rockets could produce a more capable missile defense within an acceptable cost range that could eliminate or greatly reduce the need for fallout shelters. As part of its Homeland Defense responsibilities, USNORTHCOM could lend its voice to those already advocating for an upgraded and improved national missile defense capability.
Considering the previously identified options, we recommend the following actions to help attain the desired end state for 21st Century Civil Defense.

1. **Preparation for Nationwide Disaster.** The National Disaster Recovery Framework, and electricity, nuke, and cyber incident annexes are all predicated on the ability to call on Federal resources following a disaster. Given FEMA's experience responding in rapid succession to hurricanes Harvey, Irma, and Maria in 2017, it seems unlikely that any Federal support will be available following a nationwide disaster. FEMA should use HSGP funding to prioritize a national series of exercises at all levels of government examining response and recovery from a Black Sky Event in which no other State or Federal support would be forthcoming annually.

2. **National Sheltering Program.** Fallout shelters are no more available today than they were during the Cold War, and probably less so. Only public support and Congress can fix that. However, just as dual-use applications facilitated public acceptance of CD programs during the Cold War, FEMA could investigate alternatives that might offer similar public appeal to assist with advising the White House and Congress. FEMA's Building Resilient Infrastructure and Communities grant funding, Building Codes Strategy, Hazard Mitigation Grant Program, Public Assistance Program, and Safe Room Program offer readily accessible means to incorporate

Fallout Shelter design, planning, construction, and national requirements for urban planning and guidance into existing FEMA mechanisms.

3. **National Evacuation Program.** Urban evacuation is a lesser substitute for sheltering from nuclear attack, however it remains a viable and quicker alternative. FEMA cannot dictate emergency response strategy. That is for States to choose. However, FEMA can advise States and perhaps sponsor a series of workshops to help them develop strategy for protecting their populations from nuclear attack. Evacuations have historically been successfully conducted, most famously for Civil Defense in 1955 in Portland, Oregon "Operation Greenlight" in which 100,000 of the target population were able to evacuate in 34 minutes. Present-day the practice for mass evacuation is regular practice, especially among large communities and disaster-prone populations. With additional national exercise program planning, funding, community education and training this presents a viable option dependent upon the factor of time.

4. **Public Education Curriculum.** Public education curriculum is controlled at the State and Local level and, like Emergency Preparedness, only influences so far as Federal funding is accepted. However, FEMA can help advise the Education Department regarding minimum requirements for sponsored Civics programs addressing individual Emergency Preparedness fundamentals.

5. **Split Civil-Military Capabilities.** President Kennedy viewed Civil Defense as a military responsibility and subsequently split CD responsibilities between the White House and Pentagon. Should the same be done today? It might be worth noting that all public CD exercises ended after this split. Today, FEMA oversees a robust disaster exercise program. There is no perceived benefit to splitting responsibilities, and it would only increase the burden on DoD to try and match programs already in effect.

6. **National Guard Disposition.** Without Federal or State support following a disaster, States will be hard pressed to deliver basic goods and services to their citizens. The National Guard will be indispensable to this task. But what if, as Mr. Lucie conjectures, the US military is mobilized to deploy overseas following an attack? The National Guard also plays a large role as part of the nation's Total Force. Who would have precedent, the Governors or the President? This topic needs to be explored, and if it already has, it needs to be revisited and refreshed. FEMA could assist USNORTHCOM with addressing this issue with the States.

7. **Civil Defense Priorities.** After completing his thorough analysis of contemporary Civil Defense requirements, Mr. Lucie proposed a set of priorities to help re-establish national readiness. We have noted that Mr. Lucie's priorities contain a dependent relationship whereby the last two cannot be ensured unless the first is. To fix this, we recommend an alternative set of priorities we think are more practical and better conform with the findings of this study:

   CD Priority 1: FEMA sponsor periodic State exercises evaluating Infrastructure Recovery.
   CD Priority 2: FEMA sponsor periodic State exercises evaluating Black Sky Events.
   CD Priority 3: FEMA sponsor periodic State exercises evaluating Continuity of Government.
   CD: Priority 4: DHS, FEMA, CISA, USNORTHCOM in partnership with the National Security Council develop a National Planning Framework and new guiding policy and doctrine focused specifically on Civil Defense to foster a shared understanding of roles and responsibilities during

wartime incidents across all levels of government, including state, tribal, local, territorial, including the private sector.

Opportunities

Future Funding, Research, Partnership, Planning & Preparedness Activities

This report highlights key areas of homeland defense and civil defense examined and evaluated against historical programs and responses from past wars such as World War I, World War II, and the Cold War to inform posturing for present and future conflicts in the 21st Century. The reemergence of the threat of full nuclear war with Russia, complex physical and cyber-attacks, EMP's both naturally occurring resultant from space weather, and/or adversarial capabilities in addition to rising geopolitical conflicts and territorial aggression from rogue and state actors such as China and North Korea call for re-establishment of long abandoned and disregarded civil defense policy and the establishment of new civil defense doctrine in response. Every topic within this report is an area that is critical for further exploration, expansion, and inquiry. Each domain within civil defense is expansive and should be further examined. Chief among the opportunities that exist is the clear demonstrated need for extensive further funding, research, partnership, and development of plans and exercises that specifically address civil defense as it pertains to the United States and its territories. DHS, FEMA, CISA, USNORTHCOM in partnership with the National Security Council are strongly recommended to develop a National Planning Framework and new guiding policy and doctrine focused specifically on Civil Defense to foster a shared understanding of roles and responsibilities during wartime incidents across all levels of government, including state, tribal, local, territorial, including the private sector.

Establish Civil Defense Center of Excellence

Civil Defense has long been a disregarded legacy function of DHS, FEMA, and emergency management. The establishment of a Center of Excellence to better coordinate regional protection, preparedness, mitigation, resilience and thought leadership cultivation, adaption, innovation, and multi-sector, interdisciplinary partnerships, the establishment of a joint-defense USNORTHCOM-HDI, and DHS-FEMA funded, Center of Excellence should be established to allow for multiple entities, colleges, universities, researchers, interdisciplinary research teams, private sector entities, cleared defense industry partners, emergency mangers, individuals, military students, and government agency partners (USNORTHCOM, HDI, DHS, CISA, EMI, NPS, DHS S&T, etc.) to synergize efforts along key lines of research and inquiry. There are a number of models and means to efficiently accomplish this utilizing existing mechanisms with expanded funding support. This recommendation includes hosting the Center of Excellence within a university or suitable institute such as the USAFA, Homeland Defense Institute, and/or the Naval Postgraduate School, Center for Homeland Defense and Security. Typically, centers of excellence are university-led in partnership with its sponsoring agencies. Membership should be open and non-restricted to invite wide participation and equitable access to collaborate in developing civil defense solutions as these programs will ultimately impact all aspects and sectors of the country during wartime incidents.

Summary

Homeland Defense and Civil Defense share a similar strategy, resilience. Homeland Defense and Civil Defense also share a causal relationship: Civil Defense is what happens when Homeland Defense

fails. This does not mean they can't be mutually supporting. USNORTHCOM can work with FEMA to enhance State and Local resilience following nationwide attack, and in return, improved resilience can raise a potential attacker's opportunity costs and reduce their expected benefits to help deter attack on the US homeland.

Conclusion

The world watches with concern as events unfold in Ukraine and around the world. The US maintains vigilance and deterrence to help protect its citizens from those who would do them harm. Once again we find ourselves living under the uncertainty of nuclear war. If there is room for hope, though, it is in the fact we have not resumed an ideological competition. This crisis is the making of a single person and some day that person will be gone. Until that day, we must prepare for a potentiality that nobody wants to see happen.

About Simental Industries Ltd.

Simental Industries Ltd. is a Homeland Security & Emergency Management Consulting Firm and Disaster Research Collaborative. Our work spans the Homeland Security Enterprise.

Simental Industries Ltd. mission is to lead cutting edge research and science to develop new, innovative systems, technologies and solutions for the Homeland Security Enterprise. Our goal is to develop solutions that make the world resilient to crime, disasters, climate change and the environment. Solutions and products that revolutionize the way we integrate research, science, data, education, cyber and physical security, safety, emergency preparedness, disaster mitigation, climate adaptation and community resilience into our society.

Research Collaborative – SHIELD Initiative

Within Simental Industries is the ***Strategic Homeland Security Enterprise Research Initiative - SHIELD Initiative.*** The SHIELD Initiative is a voluntary ***research collaborative*** focused on exploring the forefront of research, science, technology, and innovation for the homeland security enterprise. Our goal is to bring together practitioners, academicians, and industry to push thought leadership and exploration in critical areas to revolutionize how we approach these topics in the homeland security enterprise. We aim to build a robust, inclusive community of partners and become a force multiplier in homeland security research. In our own efforts to become part of a greater community of homeland security researchers we found this to be an area that was severely lacking. The SHIELD Initiative's goal is to build diverse, cross cutting partnerships and networks across the public sector, private sector, academia and industry. Our philosophy is based on the belief that there is a place for EVERYONE in the homeland security enterprise. We hope you'll join us in confronting some of the biggest problems facing the world today.

SHIELD's strategic research focus areas serve as critical elements in our vision of the future of the homeland security enterprise. This research, when realized will shield and safeguard communities for generations to come. Envisioned in our motto in Latin, "Per Scientia, Salus, Securitas et mollitiam" which means "Through Science, Safety, Security and Resilience".

Project Team

Principal Investigator
Dr. Rick White, PhD, USAF Ret.
Adjunct Professor, Tulane University
Lead Security Engineer & Chief Research Partner,
Simental Industries Ltd. – Shield Initiative
rwhite3572@gmail.com

Co-Principal Investigator
Mr. Arthur J. Simental, M.S., CEM
Adjunct Instructor & SME – Homeland Security & Emergency Management,
Colorado Technical University
Director of Emergency Management
University of Colorado Colorado Springs
Founder & CEO, Simental Industries Ltd. – Shield Initiative
arthur@simentalindustries.com

Co-Principal Investigator
Mr. John Holst, M.S., USAF vet
Chief Editor, Ill Defined Space
Chief Research Partner Space & Defense,
Simental Industries Ltd. – Shield Initiative
space.operations.pro@outlook.com

Research Fellow
Erin Christon, M.A.
Recent Graduate – Research and Evaluation Methods
University of Colorado Denver
Simental Industries Ltd. – Shield Initiative
erin.christon@outlook.com

About the Authors

Dr. Rick White, PhD, USAF Ret.
Dr. White is a retired Air Force officer and semi-retired university professor living in Colorado Springs. During his twenty-year Air Force career he served as a programmer analyst, network engineer, software engineer, Communications Director for Operation Provide Comfort, Deputy Communications Commander for Cheyenne Mountain, and professor of military studies at the Air Force Academy. He earned his Ph.D. in Engineering Security and conducted research for the Department of Homeland Security while advancing game-based teaching techniques at UCCS. He also spent three years as an exercise developer for USNORTHCOM. He now consults and teaches emergency planning for Tulane.

Mr. Arthur J. Simental, M.S., CEM
Mr. Arthur J. Simental is a Homeland Security & Emergency Management Adjunct Instructor for the College of Security Studies at Colorado Technical University. Mr. Simental is also the Founder & CEO of Simental Industries Ltd., a Homeland Security & Emergency Management Consulting Firm & Disaster Research Collaborative and is concurrently the Director of Emergency Management for the University of Colorado Colorado Springs. Mr. Simental is a former Public Health Advisor for the Centers for Disease Control and Prevention, Division of Global Migration and Quarantine, Quarantine and Border Health Services Branch – Quarantine Service where he spent the last two years supporting the Epidemiology Field Team and the Los Angeles Quarantine Station working on the federal COVID-19 response, Operation Allies Welcome in Colorado, Monkeypox, and severed on various teams in support of numerous public health emergency responses. Mr. Simental has fourteen years of service in Government, Homeland Security & Emergency Management and Emergency Services. Serving at the local, county, regional, state, federal level, and in the private and non-profit sectors in homeland security, emergency management, healthcare & public health emergency preparedness, space & defense, security, education and critical infrastructure. Mr. Simental is also a homeland security researcher, published author, former Department of Defense National Security Innovation Network – Hirethon Ambassador, Certified Threat Liaison Officer with the Colorado Information and Analysis Center, a Member of FEMA's Science, Technology and Integration Special Interest Group, FEMA's Resilient Nation Partnership Network, and Certified Emergency Manager with the International Association of Emergency Managers. Mr. Simental earned a Master of Science in Homeland Security, Emergency Management and Public Health from Colorado Technical University. Presently, Mr. Simental is a second-year doctoral student, pursuing a Doctor of Management in Homeland Security from CTU. Mr. Simental has published on various topics spanning homeland security, emergency management, disaster resilience, climate adaptation, space technology & innovations, public health & healthcare emergency preparedness, and others.

Mr. John Holst, M.S., USAF Ret.
John Holst's focus on space threads throughout his work history. He places an importance on space and space activities, but also believes that neither one stands apart from the realities of space business and the challenges of space. He researches those aspects, questions his findings, and then writes about them. For Mr. Holst, space activities and technologies are accomplished and provided to improve the lives of humans everywhere. Nearly ten years ago, Mr. Holst started using his natural analytical and research talent in addition to his writing ability while working for the Space Foundation, Quilty Analytics, and his own business (Ill-Defined Space). Since 2014, Mr. Holst's work has been and continues to be

published in the Space Foundation's annual publication, "The Space Report." Since 2014, he's researched the global space industry and written about it in non-profit, for-profit, and other roles. Mr. Holst continues that now, currently writing analyses for his site, Ill-Defined Space, as well as for companies such as Astralytical, Orbify, and Simental Industries. Before his research roles, he worked for five+ years providing direct support to the Missile Defense Agency's (MDA) Ballistic Missile Defense System Test Program/Directorate for Test. While he started as a Battle Rhythm Coordinator, Mr. Holst expanded from that within a year of his employment in the MDA, working for Sparta/Cobham at the time. He ultimately ended up working for the University Affiliated Research Center, Space Dynamics Laboratory, working on the STSS program. Prior to working with the MDA, Mr. Holst served in the United States Air Force (USAF). He gained 11 years of extensive leadership experience in the USAF as an officer and Space Operator. Mr. Holst started as a "missileer"—a Deputy Missile Combat Crew Commander. He progressed, eventually training other missileers, first in Minot AFB, ND, then in Vandenberg AFB, CA for onboarding new officer missileers. Afterward, Mr. Holst was assigned to Denver, ultimately working as a National Space Systems Operations Director.

Erin Christon, M.A.

Erin recently graduated over the summer of 2022 from the University of Colorado – Denver with a Master's degree in Research and Evaluation Methods. Erin has an education and research background working with diverse populations, minorities, undeserved communities and advancing and advocating work in equity, diversity, inclusion and access. Erin has also been supporting Team Rubicon with wildfire mitigation.

Acronyms

ABM	Anti-Ballistic Missile
ABNCP	Airborne Command Post
AFNORTH	Air Forces North
AOR	Area of Responsibility
APS	American Physical Society
ARNORTH	Army North
ARPA	Advanced Research Projects Agency (forerunner to DARPA)
BMD	Ballistic Missile Defense
BMDO	Ballistic Missile Defense Organization
BRI	Belt & Road Initiative
BSE	Black Sky Event
C3	Command, Control, and Communications
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance
CBRN	Chemical, Biological, Radiological, & Nuclear
CCDR	Combatant Commander
CCP	Chinese Communist Party
CD	Civil Defense
CERT	Computer Emergency Readiness Team
CFB	Canadian Forces Base
CFR	Code of Federal Regulations
CG	Commanding General
CINC	Commander in Chief
CINCAL	Commander in Chief Alaskan Command
CINCARIB	Commander in Chief Caribbean Command
CINCEUR	Commander in Chief European Command
CINCFE	Commander in Chief Far East Command
CINCLANTFLT	Commander In Chief Atlantic Fleet
CINCNE	Commander in Chief Northeast Command
CINCPAC	Commander in Chief Pacific Command
CIP	Critical Infrastructure Protection
CMF	Cyber Mission Force
CNO	Chief of Naval Operations
CO	Cyberspace Operations
COG	Continuity of Government
COG	Global Operations Center
COMUSNAVNORTH	Commander United States Naval Forces for Northern Command
CONAD	Continental Air Defense Command
CONUS	Continental United States
COOP	Continuity of Operations
COP	Common Operating Picture
CPG-201	Comprehensive Preparedness Guide 201
CRP	Crisis Relocation Program
CSZ	Cascadia Subduction Zone
DCO	Defensive Cyber Operations
DCPA	Defense Civil Preparedness Agency
DHS	Department of Homeland Security
DOD	Department of Defense
DODIN	Department of Defense Information Network
DoE	Department of Energy
DPRK	Democratic People's Republic of Korea
DSCA	Defense Support of Civil Authorities
ECG	Enduring Constitutional Government
E-ISAC	Electricity Information Sharing and Analysis Center

EMAC	Emergency Management Assistance Compact
EMP	Electromagnetic Pulse
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
EP	Emergency Preparedness
ESF	Emergency Support Function
EU	European Union
FCDA	Federal Civil Defense Administration
FCO	Federal Coordinating Officer
FEMA	Federal Emergency Management Agency
FIOP	Federal Interagency Operations Plans
FP	Force Protection
FRP	Federal Response Plan
GBIs	Ground Based Interceptors
GCCs	Geographic Combatant Commands
GMD	Ground-based Midcourse Defense
GWOT	Global War on Terrorism
HD	Homeland Defense
HSEEP	Homeland Security Exercise and Evaluation Program
HSGP	Homeland Security Grant Programs
HSPD-8	Homeland Security Presidential Directive #8
IADs	Integrated Air Defenses
ICBM	Inter-Continental Ballistic Missile
ICS	Incident Command System
ICS-CERT	Industrial Control Systems CERT
IEMS	Integrated Emergency Management System
IFOR	Implementation Force
JCS	Joint Chiefs of Staff
JFACC	Joint Force Air Component Commander
JFLCC	Joint Forces Land Component Commander
JFLCC	Joint Force Land Component Commander
JFMCC	Joint Force Maritime Component Commander
KMT	Kuomintang
MA	Mission Assignment
MAA	Mutual Assistance Agreement
MAD	Mutual Assured Destruction
MAD	Mutual Assured Destruction
MATO	MA Task Order
MIRV	Multiple Independently Targetable Reentry Vehicles
MND(N)	Multinational Division (North)
MSR	Missile Site Radar
NATO	North Atlantic Treaty Organization
NATO	North Atlantic Treat Organization
NCCIC	National Cybersecurity and Communications Integration Center
NCCS	Nuclear Command and Control System
NCR	National Capital Region
NDAA	National Defense Authorization Act
NDRF	National Disaster Recovery Framework
NDS	National Defense Strategy
NEF	National Essential Function
NEP	National Exercise Program
NERC	North American Electric Reliability Corporation
NGO	Non-Governmental Organization
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NMCC	National Military Command Center

NORAD	North American Aerospace Defense Command
NPEP	National Plan for Emergency Preparedness
NPF	National Planning Framework
NPG	National Preparedness Goal
NPS	National Preparedness System
NRF	National Response Framework
NRP	National Response Plan
NSA	National Security Agency
NSDM	National Security Decision Memorandum
NYPA	New York Power Authority
NYSC	New York State Contingent
OCD	Office of Civil Defense
OCDM	Office of Civil and Defense Mobilization
OCO	Offensive Cyber Operations
OEP	Office of Emergency Planning
PAR	Perimeter Acquisition Radar
PDD-63	Presidential Decision Directive #63
PRC	People's Republic of China
PREPA	Puerto Rico Electric Power Authority
PRNG	Puerto Rico National Guard
QHSR	Quadrennial Homeland Security Review
RFA	Request For Assistance
RMF	Risk Management Framework
ROC	Republic of China
RV	Reentry Vehicle
SAC	Strategic Air Command
SAC HQ	Strategic Air Command Headquarters
SAM	Surface-to-Air-Missile
SCADA	Supervisory Control and Data Acquisition
SDI	Strategic Defense Initiative
SDIO	Strategic Defense Initiative Organization
SecDef	Secretary of Defense
SFOR	Stabilization Force
SLBM	Submarine-Launched Ballistic Missile
SLTT	State, Local, Tribal, & Territorial
SLTT	State, Local, Tribal, and Territorial
SPR	Stakeholder Preparedness Review
SSBN	Ballistic Missile Submarine
TD	Territorial Defense Forces
THIRA	Threat and Hazard Identification and Risk Assessment
TRA	Taiwan Relations Act
UAF	Ukrainian Armed Forces
UCP	Unified Command Plan
UK	United Kingdom
UNSC	United Nations Security Council
USAR	United States Army Reserve
USARNORTH	Unites States Army North
USC	United States Code
USFF	United States Fleet Forces Command
USNORTHCOM	United States Northern Command
USSTRATCOM	United States Strategic Command
WEM	Wisconsin Emergency Management
WMD	Weapons of Mass Destruction

“Hope is not a strategy”
- Vince Lombardi

References

[1] R. White and J. Billups, "Homeland Security: The Five-W's," August 2020. [Online]. Available: https://sites.google.com/view/hs5ws-com/home. [Accessed December 2022].

[2] Wikipedia, the Free Encyclopedia, "2022 Russian Invasion of Ukriane," 2022. [Online]. Available: https://en.wikipedia.org/wiki/2022_Russian_invasion_of_Ukraine . [Accessed December 2022].

[3] European Parliamentary Research Service, "Russia's War on Ukraine: Military Balance of Power," European Parliament, Strausburg, France, 2022.

[4] Congressional Research Service, "Russia's War on Ukraine: U.S. Policy and the Role of Congress," Library of Congress, Washington, DC, 2022.

[5] G. Faulconbridge, "Factbox: Has Putin Threatened to Use Nuclear Weapons?," Reuters, 27 October 2022. [Online]. Available: https://www.reuters.com/world/europe/has-putin-threatened-use-nuclear-weapons-2022-10-27/. [Accessed December 2022].

[6] Central Intelligence Agency, "The World Factbook: China," December 2022. [Online]. Available: https://www.cia.gov/the-world-factbook/countries/china/. [Accessed December 2022].

[7] Central Intelligence Agency , "The World Factbook: Taiwan," December 2022. [Online]. Available: https://www.cia.gov/the-world-factbook/countries/taiwan/#military-and-security. [Accessed December 2022].

[8] Brookings Institute, "A Taiwan Perspective on What is at Stake after Nancy Pelosi's Visit to Taiwan," September 2022. [Online]. Available: https://www.brookings.edu/blog/order-from-chaos/2022/09/26/a-taiwan-perspective-on-what-is-at-stake-after-nancy-pelosis-visit-to-taiwan/. [Accessed December 2022].

[9] B. Lin and J. Wuthnow, "Pushing Back Against China's New Normal in the Taiwan Strait," Texas National Security Review, August 2022. [Online]. Available: https://warontherocks.com/2022/08/pushing-back-against-chinas-new-normal-in-the-taiwan-strait/. [Accessed December 2022].

[10] B. Lin, B. Hart, M. P. Fuaiole, S. Lu, H. Price and N. Kaufman, "Tracking the Fourth Taiwan Strait Crisis," China Power Project, October 2022. [Online]. Available: https://chinapower.csis.org/tracking-the-fourth-taiwan-strait-crisis/. [Accessed December 2022].

[11] Congressional Research Service, "North Korea: September 2022 Update," Library of Congress, Washington, DC, 2022.

[12] Congressional Research Service, "U.S.-North Korea Relations," Library of Congress, Washington, DC, 2020.

[13] D. Vergun, "DOD Official Outlines U.S. Nuclear Deterrence Strategy," U.S. Deaprtment of Defense, September 2020. [Online]. Available: https://www.defense.gov/News/News-Stories/Article/Article/2334600/dod-official-outlines-us-nuclear-deterrence-strategy/. [Accessed December 2022].

[14] R. Tiron, "Preventing Nuclear "Armageddon' Hinges on US Policy of Ambiguity," Bloomberg Government, October 2022. [Online]. Available: https://about.bgov.com/news/preventing-nuclear-armageddon-hinges-on-us-policy-of-ambiguity/. [Accessed December 2022].

[15] The White House, "The National Plan for Emergency Preparedness," Government Printing Office, Washington, DC, 1964.

[16] Electric Infrastructure Security (EIS) Council, "Black Sky Hazards," 2022. [Online]. Available: https://eiscouncil.org/black-sky/. [Accessed December 2022].

[17] Graham Commission, "Report of the Commission to Assess the Threat to the Untied States from Electromagnetic Pulse (EMP) Attack," Government Printing Office, Washington, DC, 2004.

[18] The Economist, "A Nest of Wipers," pp. 67-69, 3 December 2022.

[19] Wikipedia The Free Encyclopedia, "Colonial Pipeline Ransomware Attack," December 2022. [Online]. Available: https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack#Impact. [Accessed December 2022].

[20] U.S. Commission on Civil rights, "Civil Rights and Protections During the Federal Response to Hurricanes Harvey and Maria," Washington, DC, 2022.

[21] J. Humphrey, "7 Things About Life in Puerto Rico With No Electricity," IEEE Spectrum, 4 December 2017. [Online]. Available: https://spectrum.ieee.org/7-things-about-life-in-puerto-rico-with-no-electricity. [Accessed 31 December 2022].

[22] FEMA, "2017 Hurricane Season FEMA After-Action Report," Washington, DC, 2018.

[23] RAND Corporation, "U.S. Army North in the Hurricane Maria Response," Santa Monica, CA, 2020.

[24] New York Power Authority, "After Action Report: New York State Utility Contingent Emergency Response to Hurricane Maria," New York, NY, 2018.

[25] National Association of Regulatory Utility Commissioners, "EPRR Task A: Black Sky Playbook Use Cases," Washington, DC, 2021.

[26] C. E. Kirkpatrick, "Defense of the Americas, 7 December 1941 - 2 September 1945," US Army Center of Military History, Washington, DC, 2003.

[27] R. H. Cole, W. S. Poole, J. F. Schnabel, R. J. Watson and W. J. Webb, "The History of the Unified Command Plan 1946-993," Joint History Office of the Chairman of the Joint Chiefs of Staff, Washington, DC, 1993.

[28] US State Department, Office of the Historian, "Sputnik, 1957," [Online]. Available: https://history.state.gov/milestones/1953-1960/sputnik. [Accessed 27 March 2023].

[29] 341st Missile Wing Public Affairs, "Air Force History of ICBM Development, Safeguarding America," Malmstrom AFB, MT, 2012.

[30] Wikipedia, "UGM-27 Polaris," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/UGM-27_Polaris. [Accessed 27 March 2023].

[31] Congreassional Research Service, "US Nuclear Weapons: Changes in Policy and Force Structure," Library of Congress, Washington, DC, 2008.

[32] Wikipedia, "Nike Zeus," [Online]. Available: https://en.wikipedia.org/wiki/Nike_Zeus. [Accessed 27 March 2023].

[33] Wikipedia, "Sprint (missile)," [Online]. Available: https://en.wikipedia.org/wiki/Sprint_(missile). [Accessed 27 March 2023].

[34] Wikipedia, "Nike-X," [Online]. Available: https://en.wikipedia.org/wiki/Nike-X . [Accessed 27 March 2023].

[35] Wikipedia, "Sentinel Program," [Online]. Available: https://en.wikipedia.org/wiki/Sentinel_program . [Accessed 27 March 2023].

[36] Wikipedia, "Safeguard Program," [Online]. Available: https://en.wikipedia.org/wiki/Safeguard_Program. [Accessed 27 March 2023].

[37] Wikipedia, "Strategic Defense Initiative," [Online]. Available: https://en.wikipedia.org/wiki/Strategic_Defense_Initiative. [Accessed 27 March 2023].

[38] Atomic Heritage Foundation, "Strategic Defense Initiative (SDI)," 18 July 2018. [Online]. Available: https://ahf.nuclearmuseum.org/ahf/history/strategic-defense-initiative-sdi/. [Accessed 27 March 2023].

[39] Wikipedia, "List of Nuclear Close Calls," [Online]. Available: https://en.wikipedia.org/wiki/List_of_nuclear_close_calls. [Accessed 27 March 2023].

[40] Wikipedia, "Gulf War," [Online]. Available: https://en.wikipedia.org/wiki/Gulf_War . [Accessed 28 March 2023].

[41] Wikipedia, "Operation Provide Comfort," [Online]. Available: https://en.wikipedia.org/wiki/Operation_Provide_Comfort. [Accessed 28 March 2023].

[42] Wikipedia, "Iraqi No-Fly Zones," [Online]. Available: https://en.wikipedia.org/wiki/Iraqi_no-fly_zones_conflict. [Accessed 28 March 2023].

[43] Wikipedia, "Operation Provide Promise," [Online]. Available: https://en.wikipedia.org/wiki/Operation_Provide_Promise. [Accessed 28 March 2023].

[44] Wikipedia, "Operation Deny Flight," [Online]. Available: https://en.wikipedia.org/wiki/Operation_Deny_Flight. [Accessed 28 March 2023].

[45] Wikipedia, "Battle of Mogadishu (1993)," [Online]. Available: https://en.wikipedia.org/wiki/Battle_of_Mogadishu_(1993). [Accessed 28 March 2023].

[46] Wikipedia, "Operation Uphold Democracy," [Online]. Available: https://en.wikipedia.org/wiki/Operation_Uphold_Democracy. [Accessed 28 March 2023].

[47] Wikipedia, "Operation Deliberate Force," [Online]. Available: https://en.wikipedia.org/wiki/Operation_Deliberate_Force. [Accessed 28 March 2023].

[48] GlobalSecurity.org, "Operation Joint Endeavor," [Online]. Available: https://www.globalsecurity.org/military/ops/joint_endeavor.htm. [Accessed 28 March 2023].

[49] Wikipedia, "NATO Bombing of Yugoslavia," [Online]. Available: https://en.wikipedia.org/wiki/NATO_bombing_of_Yugoslavia. [Accessed 28 March 2023].

[50] R. White, Homeland Defense, An Overview, Colorado Springs, CO: Pearson Custom Publishing, 2007.

[51] Chairman of the Joint Chiefs of Staff, "Joint Publication 1, Doctrine for the Armed Forces of the United States," Washington, DC, 2017.

[52] Chairman of the Joint Chiefs of Staff, "JP 3-27, Homeland Defense," Pentagon, Arlington, VA, 2018.

[53] US Cyber Command, "CYBER 101 - Cyber Mission Force," 1 November 2022. [Online]. Available: https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/. [Accessed 29 March 2023].

[54] Wikipedia, "United States Strategic Command," [Online]. Available: https://en.wikipedia.org/wiki/United_States_Strategic_Command. [Accessed 29 March 2023].

[55] Congressional Research Service, "Defense Primer: Command and Control of Nuclear Forces," Library of Congress, Washington, DC, 2022.

[56] US Department of Defense, "National Defense Strategy," Pentagon, Arlington, VA, 2022.

[57] Q. Lucie, "How FEMA Could Lose America's Next Great War," *Homeland Security Affairs,* vol. 15, p. Article 1, 2019.

[58] DHS National Preparedness Task Force, "Civil Defense and Homeland Security: A Short History of National Preparedness Efforts," US Department of Homeland Security, Washington, DC, 2006.

[59] P. G. W. Bush, "The Department of Homeland Security," Washington, DC, 2002.

[60] National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report," U.S. Government Printing Office, Washington, DC, 2004.

[61] The White House, "The Federal Response to Hurricane Katrina, Lessons Learned," The White House, Washington, DC, 2006.

[62] R. P. White, "Homeland Security in a Nutshell," *International Journal of Social Science Studies,* vol. 5, no. 6, pp. 9-14, 2017.

[63] FEMA, "Guide to Continuity of Government," Washington, DC, 2021.

[64] C. Coetzee and D. van Niekerk, "Tracking the Evolution of the Disaster Management Cycle: A General System Theory Approach," *JAMBA: Journal of Disaster risk Studies,* vol. 4, no. 1, 2012.

[65] FEMA, "National Preparedness Goal," Washington, DC, 2016.

[66] FEMA, "National Disaster Recovery Framework," Washington, DC, 2016.

[67] NERC, "GridEx," [Online]. Available: https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx. [Accessed 3 January 2023].

[68] National Infrastructure Advisory Council (NIAC), "Surviving a Catastophic Power Outage," Washington, DC, 2018.

[69] FEMA, "National Level Exercise Background," [Online]. Available: https://www.fema.gov/emergency-managers/planning-exercises/nle/background. [Accessed 6 January 2023].

[70] USA FACTS, "Is the Number of Major Natural Disasters Increasing?," 5 November 2022. [Online]. Available: https://usafacts.org/articles/are-the-number-of-major-natural-disasters-increasing/. [Accessed 9 January 2023].

[71] PBS American Experience, "Operation Alert," [Online]. Available: https://www.pbs.org/wgbh/americanexperience/features/bomb-operation-alert/. [Accessed 5 January 2023].

[72] T. C. Davis, Stages of Emergency: Cold War Nuclear Civil Defense, Durham, NC: Duke University Press, 2007.

[73] D. Cole, "Ukraine Invasion, Russia's 226 attacks on health-care targets in Ukraine are part of a larger pattern," NPR, 2022. [Online]. Available: https://www.npr.org/sections/goatsandsoda/2022/03/16/1086982186/russias-strike-on-ukraine-maternity-hospital-is-part-of-a-terrible-wartime-tradi.

[74] FEMA, "Community Lifelines," 2023. [Online]. Available: https://www.fema.gov/emergency-managers/practitioners/lifelines .

[75] "Lawmakers-stage-war-game-conflict-with-china-hoping-to-deter-real-one," Voice of America, 22 04 2023. [Online]. Available: https://www.voanews.com/a/lawmakers-stage-war-game-conflict-with-china-hoping-to-deter-real-one-/7062420.html.

[76] J. Dobbins, S. G. Jones, K. Crane and B. C. DeGrasse, "The Beginner's Guide to Nation-Building," RAND Corportation, Santa Monica, 2007.

[77] J. Burgess and J. Harness, "No power in Ukraine's second city after Russian strikes," BBC, 16 December 2022. [Online]. Available: https://www.bbc.com/news/live/world-europe-63998267. [Accessed 5 May 2023].

[78] T. Hitchens, "SpaceX didn't intend that Starlink be 'weaponized' by Ukraine: Shotwell," Breaking Media, 8 February 2023. [Online]. Available: https://breakingdefense.com/2023/02/spacex-didnt-intend-that-starlink-be-weaponized-by-ukraine-shotwell/. [Accessed 5 May 2023].

[79] B. Clark, "The Fall and Rise of Russian Electronic Warfare," Hudson Institute, Inc., 30 July 2022. [Online]. Available: https://www.hudson.org/national-security-defense/the-fall-and-rise-of-russian-electronic-warfare. [Accessed 5 May 2023].

[80] Gunter's Space Page, "Orbital Launches of 2012," Gunter's Space Page, 19 February 2023. [Online]. Available: https://space.skyrocket.de/doc_chr/lau2012.htm. [Accessed 5 May 2023].

[81] Gunter's Space Page, "Orbital Launches of 2022," Gunter's Space Page, 24 April 2023. [Online]. Available: https://space.skyrocket.de/doc_chr/lau2022.htm. [Accessed 5 May 2023].

[82] J. Brodkin, "Starlink's new Dishy McFlatface is smaller and lighter, still costs $499," Wired Media Group, 12 November 2021. [Online]. Available: https://arstechnica.com/information-technology/2021/11/starlink-unveils-2nd-generation-satellite-dish-and-new-wi-fi-router/?comments=1&comments-page=1. [Accessed 5 May 2023].

[83] Skyfi, "Pricing," Skyfi, 2023. [Online]. Available: https://www.skyfi.com/pricing. [Accessed 5 May 2023].

[84] CFSCC CJ3/6, "Space-Track.org," United States Air Force, 2023. [Online]. Available: Space-track.com. [Accessed 5 May 2023].

[85] J. A. Guerrero-Saade and M. van Amerongen, "AcidRain | A Modem Wiper Rains Down on Europe," SentinelOne, 31 March 2022. [Online]. Available: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/. [Accessed 5 May 2023].

[86] J. Pearson, R. Satter, C. Bing and J. Schectman, "Exclusive: U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say," Reuters, 11 March 2022. [Online]. Available: https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/. [Accessed 5 May 2023].

[87] Union of Concerned Scientists, "UCS Satellite Database," Union of Concerned Scientists, 1 May 2022. [Online]. Available: https://www.ucsusa.org/resources/satellite-database. [Accessed 5 May 2023].

[88] O. Stashevskyi and F. Bajak, "They’re jamming everything: How secretive electronic warfare shapes war in Ukraine," The Times of Israel, 3 June 2022. [Online]. Available: https://www.timesofisrael.com/theyre-jamming-everything-secretive-electronic-warfare-shapes-war-in-ukraine/. [Accessed 5 May 2023].

[89] D. Axe, "https://www.forbes.com/sites/davidaxe/2021/11/23/russias-jamming-force-could-isolate-ukrainian-troops-so-artillery-can-destroy-them/?sh=37ea5af72015," Forbes, 23 November 2021. [Online]. Available: https://www.forbes.com/sites/davidaxe/2021/11/23/russias-jamming-force-could-isolate-ukrainian-troops-so-artillery-can-destroy-them/?sh=37ea5af72015. [Accessed 5 May 2023].

[90] C. Miller, M. Scott and B. Bender, "How Elon Musk’s space satellites changed the war on the ground," Politico, 8 June 2022. [Online]. Available: https://www.politico.eu/article/elon-musk-ukraine-starlink/. [Accessed 5 May 2023].

[91] Outlook Web Desk, "Explained: How Starlink Of Elon Musk Prevented Russian Electromagnetic Attack In Ukraine," Outlook Publishing India Pvt. Ltd, 23 April 2022. [Online]. Available: https://www.outlookindia.com/international/spacex-countered-russia-s-electromagnetic-warfare-in-ukraine-faster-than-us-military-pentagon-news-192868. [Accessed 5 May 2023].

[92] J. Trevithick, "https://www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics-including-radio-virus," Recurrent Ventures, 30 October 2019. [Online]. Available: https://www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics-including-radio-virus. [Accessed 5 May 2023].

[93] M. Bruno, "“Uber For Artillery” – What is Ukraine’s GIS Arta System?," Iconoclast Digital Services, 2022. [Online]. Available: https://themoloch.com/conflict/uber-for-artillery-what-is-ukraines-gis-arta-system/. [Accessed 5 May 2023].

[94] D. T. Burbach, "Early lessons from the Russia-Ukraine war as a space conflict," Atlantic Council, 30 August 2022. [Online]. Available: https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/early-lessons-from-the-russia-ukraine-war-as-a-space-conflict/. [Accessed 5 May 2023].

[95] M. Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine," Condé Nast Britain, 23 March 2022. [Online]. Available: https://www.wired.co.uk/article/viasat-internet-hack-ukraine-russia. [Accessed 5 May 2023].

[96] D. Swinhoe, "Satellite outage impacts more than 5,000 wind turbines across Europe," Data Centre Dynamics Ltd, 1 March 2022. [Online]. Available: https://www.datacenterdynamics.com/en/news/satellite-outage-impacts-more-than-5000-wind-turbines-across-europe/. [Accessed 5 May 2023].

[97] M. Willuhn, "Satellite cyber attack paralyzes 11GW of German wind turbines," PV Magazine, 1 March 2022. [Online]. Available: https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/. [Accessed 5 May 2023].

[98] R. Santamarta, "VIASAT incident: from speculation to technical details.," Reversemode, 31 March 2022. [Online]. Available: https://www.reversemode.com/2022/03/viasat-incident-from-speculation-to.html. [Accessed 5 May 2023].

[99] G. Graff, "The US Watches Warily for Russia-Ukraine Tensions to Spill Over," Condé Nast, 15 February 2022. [Online]. Available: https://www.wired.com/story/russia-ukraine-cyberattacks-spillover/. [Accessed 5 May 2023].

[100] E. Nakashima, "Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say," The Washington Post, 24 March 2022. [Online]. Available: https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/. [Accessed 5 May 2023].

[101] HawkEye 360, "HAWKEYE 360 SIGNAL DETECTION REVEALS GPS INTERFERENCE IN UKRAINE," HawkEye 360, 4 March 2022. [Online]. Available: https://www.he360.com/hawkeye-360-signal-detection-reveals-gps-interference-in-ukraine/. [Accessed 5 May 2023].

[102] R. Browne, "Russia jammed GPS during major NATO military exercise with US troops," Cable News Network, 14 November 2018. [Online]. Available: https://www.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html. [Accessed 5 May 2023].

[103] BBC, "Study maps 'extensive Russian GPS spoofing'," BBC, 2 April 2019. [Online]. Available: https://www.bbc.com/news/technology-47786248. [Accessed 5 May 2023].

[104] E. Jeffs, "L'Indro: Russian Threats to GPS," NextNav, 8 December 2022. [Online]. Available: https://nextnav.com/lindro-russia-gps-article-ganesh/. [Accessed 5 May 2023].

[105] Avia.Pro, "APU found ways to bypass GPS jamming over Ukraine," Avia.Pro, 19 December 2022. [Online]. Available: https://avia-pro.net/news/vsu-nashli-sposoby-oboyti-podavlenie-gps-nad-ukrainoy. [Accessed 5 May 2023].

[106] M. Meaker, "High Above Ukrain, Satellites Get Embroiled in the War," Conde Nast, 4 March 2022. [Online]. Available: https://www.wired.com/story/ukraine-russia-satellites/. [Accessed 5 May 2023].

[107] T. Withington, "No Direction Home – GPS Jamming and Avoidance Around Modern Warzones," Forecast International, 23 August 2022. [Online]. Available: https://dsm.forecastinternational.com/wordpress/2022/08/23/no-direction-home-gps-jamming-and-avoidance-around-modern-warzones/. [Accessed 5 May 2023].

[108] K. Johnson, "Airlines Report Russian GPS Jamming In Four Regions," Flying Media, 1 April 2022. [Online]. Available: https://www.flyingmag.com/airlines-report-russian-gps-jamming-in-four-regions/. [Accessed 5 May 2023].

[109] European Union Aviation Safety Agency, "Global Navigation Satellite System Outage Leading to Navigation/Surveillance Degradation," 17 March 2022. [Online]. Available: https://ad.easa.europa.eu/blob/EASA_SIB_2022_02.pdf/SIB_2022-02_1. [Accessed 5 May 2023].

[110] Reuters Staff, "CORRECTED-Finland detects GPS disturbance near Russia's Kaliningrad," Reuters, 9 March 2022. [Online]. Available: https://www.reuters.com/article/ukraine-crisis-finland-gps-idUSL5N2VB4KS. [Accessed 5 May 2023].

[111] M. Burgess, "GPS Signals Are Being Disrupted in Russian Cities," Conde Nast, 15 December 2022. [Online]. Available: https://www.wired.com/story/gps-jamming-interference-russia-ukraine/. [Accessed 5 May 2023].

[112] G. Corfield, "Russia spoofed AIS data to fake British warship's course days before Crimea guns showdown," situation publishing, 24 June 2021. [Online]. Available: https://www.theregister.com/2021/06/24/russia_ais_spoofing/. [Accessed 5 May 2023].

[113] E. Braw, "Sanction-Busting Russian Ships Are Going Under the Radar," Foreign Policy, 14 December 2022. [Online]. Available: https://foreignpolicy.com/2022/12/14/sanction-busting-russian-ships-automatic-identification-system-radar/. [Accessed 5 May 2023].

[114] R. Ranjan, "Russia Announces Space War On Elon Musk's Starlink Satellites, Accepts Moskva Was Attacked," Republic, 16 April 2022. [Online]. Available: https://www.republicworld.com/world-news/russia-ukraine-crisis/russia-announces-space-war-on-elon-musks-starlink-satellites-accepts-moskva-was-attacked-articleshow.html. [Accessed 5 May 2023].

[115] BBC, "Ukraine war: Soledar devastation revealed in satellite images," BBC, 12 January 2023. [Online]. Available: https://www.bbc.com/news/world-europe-64250202. [Accessed 5 May 2023].

[116] Amazon Staff, "https://www.aboutamazon.com/news/innovation-at-amazon/amazons-project-kuiper-satellites-will-fly-on-the-new-vulcan-centaur-rocket-in-early-2023," Amazon.com, 12 October 2022. [Online]. Available: https://www.aboutamazon.com/news/innovation-at-amazon/amazons-project-kuiper-satellites-will-fly-on-the-new-vulcan-centaur-rocket-in-early-2023. [Accessed 5 May 2023].

[117] T. Reid, "Launching Xona’s Ravens: Commercial Satnav from LEO," Inside GNSS Media & Research LLC, 18 May 2022. [Online]. Available: https://insidegnss.com/launching-xonas-ravens-commercial-satnav-from-leo/. [Accessed 5 May 2023].

[118] Planet Labs PBC, "Introducing the Pelican Constellation," Planet Labs PBC, 2023. [Online]. Available: https://www.planet.com/products/pelican/. [Accessed 5 May 2023].

"Ronald Reagan won the Cold War without firing a shot."
-Margaret Thatcher.