http://www.newyorker.com/news/news-desk/world-war-three-by-mistake

World War Three, by Mistake

Harsh political rhetoric, combined with the vulnerability of the nuclear command-and-control system, has made the risk of global catastrophe greater than ever.

By Eric Schlosser

December 23, 2016

On June 3, 1980, at about two-thirty in the morning, computers at the National Military Command Center, beneath the Pentagon, at the headquarters of the North American Air Defense Command (NORAD), deep within Cheyenne Mountain, Colorado, and at Site R, the Pentagon's alternate command post center hidden inside Raven Rock Mountain, Pennsylvania, issued an urgent warning: the Soviet Union had just launched a nuclear attack on the United States. The Soviets had recently invaded Afghanistan, and the animosity between the two superpowers was greater than at any other time since the Cuban Missile Crisis.

U.S. Air Force ballistic-missile crews removed their launch keys from the safes, bomber crews ran to their planes, fighter planes took off to search the skies, and the Federal Aviation Administration prepared to order every airborne commercial airliner to land.

President Jimmy Carter's national-security adviser, Zbigniew Brzezinski, was asleep in Washington, D.C., when the phone rang. His military aide, General William Odom, was calling to inform him that two hundred and twenty missiles launched from Soviet submarines were heading toward the United States. Brzezinski told Odom to get confirmation of the attack. A retaliatory strike would have to be ordered quickly; Washington might be destroyed within

minutes. Odom called back and offered a correction: twenty-two hundred Soviet missiles had been launched.

Brzezinski decided not to wake up his wife, preferring that she die in her sleep. As he prepared to call Carter and recommend an American counterattack, the phone rang for a third time. Odom apologized—it was a false alarm. An investigation later found that a defective computer chip in a communications device at NORAD headquarters had generated the erroneous warning. The chip cost forty-six cents.

A similar false alarm had occurred the previous year, when someone mistakenly inserted a training tape, featuring a highly realistic simulation of an all-out Soviet attack, into one of NORAD's computers. During the Cold War, false alarms were also triggered by the moon rising over Norway, the launch of a weather rocket from Norway, a solar storm, sunlight reflecting off high-altitude clouds, and a faulty A.T. & T. telephone switch in Black Forest, Colorado.

My book "Command and Control" explores how the systems devised to govern the use of nuclear weapons, like all complex technological systems, are inherently flawed. They are designed, built, installed, maintained, and operated by human beings. But the failure of a nuclear command-and-control system can have consequences far more serious than the crash of an online dating site from too much traffic or flight delays caused by a software glitch. Millions of people, perhaps hundreds of millions, could be annihilated inadvertently. "Command and Control" focusses on near-catastrophic errors and accidents in the arms race between the United States and the Soviet Union that ended in 1991. The danger never went away. Today, the odds of a nuclear war being started by mistake are low—and yet the risk is growing, as the United States and Russia drift toward a new cold war. The other day, Senator John McCain called Vladimir Putin, the President of the Russian Federation, "a thug, a bully, and a murderer," adding that anyone who "describes him as anything else is lying." Other members of Congress have attacked Putin for trying to influence the Presidential election. On Thursday, Putin warned that Russia would "strengthen the military potential of strategic nuclear forces," and President-elect Donald Trump has responded with a vow to expand America's nuclear arsenal. "Let it be an arms race," Trump told one of the co-hosts of MSNBC's "Morning Joe." "We will outmatch them at every pass and outlast them all."

The harsh rhetoric on both sides increases the danger of miscalculations and mistakes, as do other factors. Close encounters between the military aircraft of the United States and Russia have become routine, creating the potential for an unintended conflict. Many of the nuclear-weapon systems on both sides are aging and obsolete. The personnel who operate those systems often suffer from poor morale and poor training. None of their senior officers has firsthand experience making decisions during an actual nuclear crisis. And today's command-and-control systems must contend with threats that barely existed during the Cold War: malware, spyware, worms, bugs, viruses, corrupted firmware, logic bombs, Trojan horses, and all the other modern tools of cyber warfare. The greatest danger is posed not by any technological innovation but by a dilemma that has haunted nuclear strategy since the first detonation of an atomic bomb: How do you prevent a nuclear attack while preserving the ability to launch one?

“The pattern of the use of atomic weapons was set at Hiroshima,” J. Robert Oppenheimer, the scientific director of the Manhattan Project, said in November, 1945, just a few months after the Japanese city’s destruction. “They are weapons of aggression, of surprise, and of terror.” Nuclear weapons made annihilation vastly more efficient. A single bomb could now destroy a target whose elimination had once required thousands of bombs. During an aerial attack, you could shoot down ninety-nine per cent of the enemy’s bombers—and the plane that you missed could obliterate an entire city. A war between two countries with nuclear weapons, like a Wild West shoot-out, might be won by whoever fired first. And a surprise attack might provide the only hope of national survival—especially for the country with an inferior nuclear arsenal.

During the same month that Oppenheimer made his remarks, Bernard Brodie, a political scientist at Yale University, proposed a theory of nuclear deterrence that has largely guided American policy ever since. Brodie argued that the threat of retaliation offered the only effective defense against a nuclear attack. “We must do what we can to reduce the advantage that might accrue to the enemy if he hit first,” Brodie wrote, after the Soviet Union had obtained its own nuclear weapons. Despite all the money spent on building nuclear weapons and delivery systems, their usefulness would be mainly psychological. “What deters is not the capabilities and intentions we have, but the capabilities and intentions the enemy thinks we have,” a classified Pentagon report explained. “The mission is persuasion.”

The fear of a surprise attack and the necessity for retaliation soon dominated the strategic thinking of the Cold War. Every year, technological advances compressed time and added more urgency to decision-making. At a top-secret briefing in 1961, Secretary of Defense Robert McNamara was told that a Soviet surprise attack on just five targets—the Pentagon, the White House, Camp David, Site R, and High Point, a bunker inside Mount Weather, Virginia—had a good chance of wiping out the civilian leadership of the United States. By striking an additional nine targets, as part of a “decapitation” attack, the Soviet Union could kill America’s military leadership as well. The Soviets might be able to destroy America’s nuclear command-and-control system with only thirty-five missiles. Under McNamara’s guidance, the Kennedy Administration sought ways to maintain Presidential control over nuclear weapons. The Pentagon deployed airborne command posts, better communications and early-warning systems, Minuteman missiles that could be quickly launched, and a large fleet of ballistic-missile submarines.

Many of these elements were put to the test during the Cuban Missile Crisis, when a series of misperceptions, miscalculations, and command-and-control problems almost started an accidental nuclear war—despite the determination of both John F. Kennedy and Nikita Khrushchev to avoid one. In perhaps the most dangerous incident, the captain of a Soviet submarine mistakenly believed that his vessel was under attack by U.S. warships and ordered the firing of a torpedo armed with a nuclear warhead. His order was blocked by a fellow officer. Had the torpedo been fired, the United States would have retaliated with nuclear weapons. At the height of the crisis, while leaving the White House on a beautiful fall evening, McNamara had a strong feeling of dread—and for good reason: “I feared I might never live to see another Saturday night.”

Today, the United States has four hundred and forty Minuteman III intercontinental ballistic missiles, sitting in underground silos scattered across the plains of Colorado, Nebraska, Wyoming, Montana, and North Dakota. The missiles are kept on alert, at all times, ready to take off within two minutes, as a means of escaping a surprise attack. Each missile carries a nuclear warhead that may be as much as thirty times more powerful than the bomb that destroyed Hiroshima. The Minuteman III was first deployed in 1970 and scheduled for retirement in the early nineteen-eighties. The age of the weapon system is beginning to show. Most of the launch complexes were built during the Kennedy Administration, to house an earlier version of the Minuteman, and some of the complexes are prone to flooding. The command centers feel like a time capsule of late-twentieth-century technology. During a recent visit to a decommissioned Minuteman site, I was curious to see the big computer still used to receive Emergency Action Messages—launch orders from the President—via landline. The computer is an I.B.M. Series/1, a state-of-the-art machine in 1976, when it was introduced. "Replacement parts for the system are difficult to find because they are now obsolete," a report by the Government Accountability Office said last May, with some understatement, about a computer that relies on eight-inch floppy disks. You can buy a smartphone with about a thousand times the memory.

The personnel who command, operate, and maintain the Minuteman III have also become grounds for concern. In 2013, the two-star general in charge of the entire Minuteman force was removed from duty after going on a drunken bender during a visit to Russia, behaving inappropriately with young Russian women, asking repeatedly if he could sing with a Beatles cover band at a Mexican restaurant in Moscow, and insulting his military hosts. The following year, almost a hundred Minuteman launch officers were disciplined for cheating on their proficiency exams. In 2015, three launch officers at Malmstrom Air Force Base, in Montana, were dismissed for using illegal drugs, including ecstasy, cocaine, and amphetamines. That same year, a launch officer at Minot Air Force Base, in North Dakota, was sentenced to twenty-five years in prison for heading a violent street gang, distributing drugs, sexually assaulting a girl under the age of sixteen, and using psilocybin, a powerful hallucinogen. As the job title implies, launch officers are entrusted with the keys for launching intercontinental ballistic missiles.

The Minuteman III is a relic of the Cold War not only in design but also in its strategic purpose. The locations of the silos, chosen more than half a century ago, make the missile useful only for striking targets inside Russia. The silos aren't hardened enough to survive a nuclear detonation, and their coördinates are well known, so the Minuteman III is extremely vulnerable to attack. The President would be under great pressure, at the outset of a war with Russia, to "use them or lose them." The missiles now have two principal roles in America's nuclear-war plans: they can be launched as part of a first strike, or they can be launched when early-warning satellites have determined that Russian warheads are heading toward the United States. After being launched, a Minuteman III cannot be remotely disabled, disarmed, or called back. From the very beginning of the Minuteman program, the Air Force has successfully fought against adding a command-destruct mechanism, fearing that an adversary might somehow gain control of it and destroy all the missiles mid-flight. "Once they're gone, they're gone," an Air Force officer told "60 Minutes" a few years ago.

The dangers of "launch-on-warning" have been recognized since the idea was first proposed, during the Eisenhower Administration. After the Cuban Missile Crisis, McNamara advised

Kennedy that the United States should never use its nuclear weapons until a nuclear detonation had occurred on American soil, and could be attributed to an enemy attack. The first Minuteman missiles had already become a great source of stress for McNamara. The control system of the original model had a design flaw: small fluctuations in the electricity entering the command center could mimic the series of pulses required by the launch switch. An entire squadron of fifty missiles might be launched accidentally without anyone turning a key. "I was scared shitless," an engineer who worked on the system later confessed. "The technology was not to be trusted." McNamara insisted that the control system be redesigned, at great expense. The destruction of fifty Soviet cities because of a mechanical glitch, a classified history of the Minuteman program later noted, would be "an accident for which a later apology might be inadequate."

The launch-on-warning policy became controversial during the nineteen-seventies, once it was publicly known. The hundreds of missiles based on American submarines, almost impossible to find in the depths of the ocean, seemed more than adequate to deter a Soviet attack. During testimony before the House Armed Services Committee in 1979, Fred Iklé, a conservative Republican who later became a top Pentagon official during the Reagan Administration, said, "If any witness should come here and tell you that a totally reliable and safe launch-on-warning posture can be designed and implemented, that man is a fool." The Pentagon repeatedly denied that launch-on-warning was American policy, claiming that it was simply one of many options for the President to consider. A recent memoir, "Uncommon Cause," written by General George Lee Butler, reveals that the Pentagon was not telling the truth. Butler was the head of the U.S. Strategic Command, responsible for all of America's nuclear weapons, during the Administration of President George H. W. Bush.

According to Butler and Franklin Miller, a former director of strategic-forces policy at the Pentagon, launch-on-warning was an essential part of the Single Integrated Operational Plan (SIOP), the nation's nuclear-war plan. Land-based missiles like the Minuteman III were aimed at some of the most important targets in the Soviet Union, including its anti-aircraft sites. If the Minuteman missiles were destroyed before liftoff, the SIOP would go awry, and American bombers might be shot down before reaching their targets. In order to prevail in a nuclear war, the SIOP had become dependent on getting Minuteman missiles off the ground immediately. Butler's immersion in the details of the nuclear command-and-control system left him dismayed. "With the possible exception of the Soviet nuclear war plan, [the SIOP] was the single most absurd and irresponsible document I had ever reviewed in my life," Butler concluded. "We escaped the Cold War without a nuclear holocaust by some combination of skill, luck, and divine intervention, and I suspect the latter in greatest proportion." The SIOP called for the destruction of twelve thousand targets within the Soviet Union. Moscow would be struck by four hundred nuclear weapons; Kiev, the capital of the Ukraine, by about forty.

After the end of the Cold War, a Russian surprise attack became extremely unlikely. Nevertheless, hundreds of Minuteman III missiles remained on alert. The Cold War strategy endured because, in theory, it deterred a Russian attack on the missiles. McNamara called the policy "insane," arguing that "there's no military requirement for it." George W. Bush, while running for President in 2000, criticized launch-on-warning, citing the "unacceptable risks of accidental or unauthorized launch." Barack Obama, while running for President in 2008, promised to take Minuteman missiles off alert, warning that policies like launch-on-warning

"increase the risk of catastrophic accidents or miscalculation." Twenty scientists who have won the Nobel Prize, as well as the Union of Concerned Scientists, have expressed strong opposition to retaining a launch-on-warning capability. It has also been opposed by former Secretary of State Henry Kissinger, former Secretary of State George Shultz, and former Senator Sam Nunn. And yet the Minuteman III missiles still sit in their silos today, armed with warheads, ready to go.

William J. Perry, who served as Secretary of Defense during the Clinton Administration, not only opposes keeping Minuteman III missiles on alert but advocates getting rid of them entirely. "These missiles are some of the most dangerous weapons in the world," Perry wrote in the *Times*, this September. For many reasons, he thinks the risk of a nuclear catastrophe is greater today than it was during the Cold War. While serving as an Under-Secretary of Defense in 1980, Perry also received a late-night call about an impending Soviet attack, a false alarm that still haunts him. "A catastrophic nuclear war could have started by accident."

Bruce Blair, a former Minuteman launch officer, heads the anti-nuclear group Global Zero, teaches at Princeton University, and campaigns against a launch-on-warning policy. Blair has described the stresses that the warning of a Russian attack would put on America's command-and-control system. American early-warning satellites would detect Russian missiles within three minutes of their launch. Officers at NORAD would confer for an additional three minutes, checking sensors to decide if an attack was actually occurring. The Integrated Tactical Warning/Attack System collects data from at least two independent information sources, relying on different physical principles, such as ground-based radar and satellite-based infrared sensors. If the NORAD officials thought that the warning was legitimate, the President of the United States would be contacted. He or she would remove the Black Book from a briefcase carried by a military aide. The Black Book describes nuclear retaliatory options, presented in cartoon-like illustrations that can be quickly understood.

Missiles launched from Russia would give the President about twenty minutes to make a decision, after consultation with the head of the U.S. Strategic Command. The President might have as few as five minutes, if missiles had been launched from Russian submarines in the western Atlantic. A decision to retaliate at once, to launch Minuteman missiles before they could be destroyed, runs the risk of killing millions of people by mistake. A decision to wait—to make sure that the attack is for real, to take no action until Russian warheads began to detonate in the United States—runs the risk losing the ability of the command-and-control system to order a retaliation. In that desperate situation, with the fate of the world in the balance, the temperament of the President would be less important than the quality of the information being offered by the system. Could you trust the sensors?

At about one-thirty in the morning, on October 23, 2010, fifty Minuteman III missiles deployed at F.E. Warren Air Force Base, in Wyoming, suddenly went offline. Launch officers could no longer communicate with their missiles. The letters "LFDN" appeared on their computer screens: Launch Facility Down. Every so often, an underground control center would lose contact with missiles, briefly. It wasn't a big deal. But having an entire squadron go down at once—and remain offline—was a highly unusual event. For almost an hour, officers tried to regain communication with the missiles. When it was reëstablished, remotely, by computer—the

control centers are miles away from the missiles—closed-circuit-television images from the silos showed that the fifty missiles were still down there. As a precaution, Air Force security officers were dispatched to all the silos in the early-morning hours.

The Air Force denied that someone had hacked into the computer network and disabled the missiles. A subsequent investigation found that a circuit card, improperly installed in a weapon-systems processor, had been dislodged by routine vibration and heat. The misalignment of the circuit card sent messages to the missiles in the wrong timing sequence. The Minuteman III's complicated launch procedures were designed to allow the missiles to be fired even if some command centers were destroyed, and to prevent rogue officers from firing them without proper authorization. As a result, the fifty missiles in each squadron are connected by coaxial cable to ten control centers, assuring redundancy and enabling one center to veto another's launch decision. Throughout the day, at designated times, each control center sends a signal to the missiles, checks their status, and receives a reply. By disrupting the time sequence, the misaligned circuit board created a cacophony of signals and blocked all communication with the missiles. The system jammed itself.

Force publicly dismissed the threat of a cyberattack on the nuclear command-and-control system, the incident raised alarm within the Pentagon about the system's vulnerability. A malfunction that occurred by accident might also be caused deliberately. Those concerns were reinforced by a Defense Science Board report in January, 2013. It found that the Pentagon's computer networks had been "built on inherently insecure architectures that are composed of, and increasingly using, foreign parts." Red teams employed by the board were able to disrupt Pentagon systems with "relative ease," using tools available on the Internet. "The complexity of modern software and hardware makes it difficult, if not impossible, to develop components without flaws or to detect malicious insertions," the report concluded.

In a recent paper for the Royal United Services Institute for Defence and Security Studies, Andrew Futter, an associate professor at the University of Leicester, suggested that a nuclear command-and-control system might be hacked to gather intelligence about the system, to shut down the system, to spoof it, mislead it, or cause it to take some sort of action—like launching a missile. And, he wrote, there are a variety of ways it might be done.

During the Cold War, as part of an espionage effort known as Project GUNMAN, Soviet agents managed to tamper with the comb-support bars in sixteen I.B.M. Selectric typewriters at the U.S. Embassy in Moscow and the U.S. Mission in Leningrad. Between 1976 and 1984, every keystroke from those typewriters was transmitted by radio to nearby Soviet listening posts. The tampering was so ingenious that it took twenty-five engineers at the National Security Agency (N.S.A.), working six days a week for several months, with X-ray equipment, to figure out how it was done. Today's integrated circuits contain billions of transistors. As the Defense Science Board notes in its report, a "subversive" chip "could destroy the processor and disable the system by simply shunting power to ground, change the processor output to incorrect results for specified inputs, or allow information leakage to the attackers." A subversive chip would look identical to a normal one.

The cybersecurity of the Minuteman III, aging and yet still on alert, is also questionable. About five thousand miles of underground cable link the control centers to the missiles, as part of the Hardened Intersite Cable System. The cable mainly traverses privately owned land. "One of the difficult parts about fixing missile cable is . . . that the wires are no longer in production," a newsletter at Minot Air Force Base explained a few years ago. The wires are copper, like old-fashioned telephone lines, surrounded by pressurized air, so that attempts to tamper with the cable can be detected. But in the early nineteen-seventies, during Operation Ivy Bells, the United States attached recording devices to similar underwater cable used by the Soviet Navy, tapping into it without piercing it. The mission was accomplished using divers and a submarine, at a depth of four hundred feet, in the Sea of Okhotsk. Digging up part of the Hardened Intersite Cable System in the middle of the night, three to eight feet under a farmer's back yard in Wyoming, would be less challenging. (The Air Force declined to comment on the specific vulnerabilities of the Minuteman III.)

Even if the hardware were pristine, malware could be inserted into the system. During Operation Orchard, in September, 2007, Israel may have hacked into Syria's early-warning system—either shutting it down completely or spoofing it into displaying clear skies—as Israeli fighters entered Syrian airspace, bombed a nuclear reactor, and flew home undetected. In 2012, the Stuxnet computer worm infiltrated computers running Microsoft Windows at nuclear sites in Iran, collected information about the industrial process there, and then issued instructions that destroyed hundreds of centrifuges enriching uranium. A similar worm could surreptitiously enter a nuclear command-and-control system, lie dormant for years, and then create havoc.

Strict precautions have been taken to thwart a cyberattack on the U.S. nuclear command-and-control system. Every line of nuclear code has been scrutinized for errors and bugs. The system is "air-gapped," meaning that its networks are closed: someone can't just go onto the Internet and tap into a computer at a Minuteman III control center. At least, that's the theory. Russia, China, and North Korea have sophisticated cyber-warfare programs and techniques. General James Cartwright—the former head of the U.S. Strategic Command who recently pleaded guilty to leaking information about Stuxnet—thinks that it's reasonable to believe the system has already been penetrated. "You've either been hacked, and you're not admitting it, or you're being hacked and don't know it," Cartwright said last year.

If communications between Minuteman control centers and their missiles are interrupted, the missiles can still be launched by ultra-high-frequency radio signals transmitted by special military aircraft. The ability to launch missiles by radio serves as a backup to the control centers—and also creates an entry point into the network that could be exploited in a cyberattack. The messages sent within the nuclear command-and-control system are highly encrypted. Launch codes are split in two, and no single person is allowed to know both parts. But the complete code is stored in computers—where it could be obtained or corrupted by an insider.

Some of America's most secret secrets were recently hacked and stolen by a couple of private contractors working inside the N.S.A., Edward Snowden and Harold T. Martin III, both employees of Booz Allen Hamilton. The N.S.A. is responsible for generating and encrypting the nuclear launch codes. And the security of the nuclear command-and-control system is being

assured not only by government officials but also by the employees of private firms, including software engineers who work for Boeing, Amazon, and Microsoft.

Lord Des Browne, a former U.K. Minister of Defense, is concerned that even ballistic-missile submarines may be compromised by malware. Browne is now the vice-chairman of the Nuclear Threat Initiative, a nonprofit seeking to reduce the danger posed by weapons of mass destruction, where he heads a task force examining the risk of cyberattacks on nuclear command-and-control systems. Browne thinks that the cyber threat is being cavalierly dismissed by many in power. The Royal Navy's decision to save money by using Windows for Submarines, a version of Windows XP, as the operating system for its ballistic-missile subs seems especially shortsighted. Windows XP was discontinued six years ago, and Microsoft warned that any computer running it after April, 2014, "should not be considered protected as there will be no security updates." Each of the U.K. subs has eight missiles carrying a total of forty nuclear weapons. "It is shocking to think that my home computer is probably running a newer version of Windows than the U.K.'s military submarines," Brown said.

In 2013, General C. Robert Kehler, the head of the U.S. Strategic Command, testified before the Senate Armed Services Committee about the risk of cyberattacks on the nuclear command-and-control system. He expressed confidence that the U.S. system was secure. When Senator Bill Nelson asked if somebody could hack into the Russian or Chinese systems and launch a ballistic missile carrying a nuclear warhead, Kehler replied, "Senator, I don't know . . . I do not know."

After the debacle of the Cuban Missile Crisis, the Soviet Union became much more reluctant to provoke a nuclear confrontation with the United States. Its politburo was a committee of conservative old men. Russia's leadership is quite different today. The current mix of nationalism, xenophobia, and vehement anti-Americanism in Moscow is a far cry from the more staid and secular ideology guiding the Soviet Union in the nineteen-eighties. During the past few years, threats about the use of nuclear weapons have become commonplace in Moscow. Dmitry Kiselyov, a popular newscaster and the Kremlin's leading propagandist, reminded viewers in 2014 that Russia is "the only country in the world capable of turning the U.S.A. into radioactive dust." The Kremlin has acknowledged the development of a nuclear torpedo that can travel more than six thousand miles underwater before devastating a coastal city. It has also boasted about a fearsome new missile design. Nicknamed "Satan 2" and deployed with up to sixteen nuclear warheads, the missile will be "capable of wiping out parts of the earth the size of Texas or France," an official news agency claimed.

The bellicose pronouncements in Moscow suggest that Russia is becoming a superpower again, modernizing its nuclear arsenal and seeking supremacy over the United States. In fact, Russia's arsenal is more inferior today and more vulnerable to a surprise attack than it was forty years ago. The Kremlin's recent propaganda brings to mind some of Nikita Khrushchev's claims from 1959: "Now we have such a stock of missiles, such an amount of atomic and hydrogen warheads, that if they attack us we could raze our potential enemies off the face of the earth." The Soviet Union did not have a single intercontinental ballistic missile when Khrushchev made those remarks.

At the moment, Russia has newer land-based missiles than the United States does, but it also has about a hundred fewer. During the Cold War, Russia possessed hundreds of mobile missiles that were hard to spot from satellites; today, it has only a hundred and fifty, which are rarely moved from their bases and more readily detected by satellite. Russia's ten ballistic-missile submarines now spend most of their time in port, where they are sitting ducks. An American surprise attack on Russian nuclear forces may have the best chance of success since the days of the Kennedy Administration. During the Cold War, as many as five warheads were targeted at each enemy missile to assure its destruction. In an age of cyber warfare, those missiles could be immobilized with just a few keystrokes. The United States Cyber Command—which reports to the U.S. Strategic Command—has been assigned the mission of using "cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities."

Russia's greatest strategic vulnerability is the lack of a sophisticated and effective early-warning system. The Soviet Union had almost a dozen satellites in orbit that could detect a large-scale American attack. The system began to deteriorate in 1996, when an early-warning satellite had to be retired. Others soon fell out of orbit, and Russia's last functional early-warning satellite went out of service two years ago. Until a new network of satellites can be placed in orbit, the country must depend on ground-based radar units. Unlike the United States, Russia no longer has two separate means of validating an attack warning. At best, the radar units can spot warheads only minutes before they land. Pavel Podvig, a senior fellow at the U.N. Institute for Disarmament Research, believes that Russia does not have a launch-on-warning policy—because its early-warning system is so limited.

According to Jeffrey Lewis, a nuclear-policy expert at the Middlebury Institute of International Studies, the deficiencies in Russia's command-and-control system feed the country's long-standing fears of encirclement by enemies ready to strike. During the twentieth century, Russia was attacked with little warning by both Germany and Japan. "I think the Russian leadership is terrified of a decapitation strike," Lewis told me recently. "Perhaps some of that is paranoia, but, on the other hand, the United States opened Operation Iraqi Freedom, in 2003, by striking Dora Farm—a failed decapitation strike against Saddam Hussein." Russia's fierce opposition to an American missile-defense system in Europe is driven by fear of the role it could play in a surprise attack. During a crisis, Russia's inability to launch on warning could raise the pressure on a Russian leader to launch without any warning. The logic of a first strike still prevails. As John Steinbruner, a renowned nuclear theorist, explained more than thirty years ago, shooting first "offers some small chance that complete decapitation will occur and no retaliation will follow. . . . [It] is probably the only imaginable route to decisive victory in nuclear war."

Vladimir Putin now wields more power over Russia's nuclear forces than any leader since Khrushchev. Putin has displayed great boldness and a willingness to take risks in foreign affairs. A surprise attack on the United States, given its nuclear superiority and largely invulnerable ballistic-missile submarines, would probably be suicidal. And yet the alternative might appear worse. Putin has described an important lesson he learned as a young man in Leningrad: "When a fight is inevitable, you have to hit first."

For the past nine years, I've been immersed in the minutiae of nuclear command and control, trying to understand the actual level of risk. Of all the people whom I've met in the nuclear realm, Sidney Drell was one of the most brilliant and impressive. Drell died this week, at the age of ninety. A theoretical physicist with expertise in quantum field theory and quantum chromodynamics, he was for many years the deputy director of the Stanford Linear Accelerator and received the National Medal of Science from Obama, in 2013. Drell was one of the founding members of JASON—a group of civilian scientists that advises the government on important technological matters—and for fifty-six years possessed a Q clearance, granting him access to the highest level of classified information. Drell participated in top-secret discussions about nuclear strategy for decades, headed a panel that investigated nuclear-weapon safety for the U.S. Congress in 1990, and worked on technical issues for JASON until the end of his life. A few months ago, when I asked for his opinion about launch-on-warning, Drell said, "It's insane, the worst thing I can think of. You can't have a worse idea."

Drell was an undergraduate at Princeton University when Hiroshima and Nagasaki were destroyed. Given all the close calls and mistakes in the seventy-one years since then, he considered it a miracle that no other cities have been destroyed by a nuclear weapon—"it is so far beyond my normal optimism." The prospect of a new cold war—and the return of military strategies that advocate using nuclear weapons on the battlefield—deeply unnerved him. Once the first nuclear weapon detonates, nothing might prevent the conflict from spiralling out of control. "We have no experience in stopping a nuclear war," he said.

During the recent Presidential campaign, the emotional stability of the Commander-in-Chief became an issue, with some arguing that a calm disposition might mean the difference between peace on Earth and a nuclear apocalypse. The President of the United States has the sole power to order the use of nuclear weapons, without any legal obligation to consult members of Congress or the Joint Chiefs of Staff. Ideally, the President would never be short-tempered, impulsive, or clinically depressed. But the mood of the Commander-in-Chief may be irrelevant in a nuclear crisis, given the current technological constraints. Can any human being reliably make the correct decision, within six minutes, with hundreds of millions of lives at stake?

Donald Trump and Vladimir Putin confront a stark choice: begin another nuclear-arms race or reduce the threat of nuclear war. Trump now has a unique opportunity to pursue the latter, despite the bluster and posturing on both sides. His admiration for Putin, regardless of its merits, could provide the basis for meaningful discussions about how to minimize nuclear risks. Last year, General James Mattis, the former Marine chosen by Trump to serve as Secretary of Defense, called for a fundamental reappraisal of American nuclear strategy and questioned the need for land-based missiles. During Senate testimony, Mattis suggested that getting rid of such missiles would "reduce the false-alarm danger." Contrary to expectations, Republican Presidents have proved much more successful than their Democratic counterparts at nuclear disarmament. President George H. W. Bush cut the size of the American arsenal in half, as did his son, President George W. Bush. And President Ronald Reagan came close to negotiating a treaty with the Soviet Union that would have completely abolished nuclear weapons.

Every technology embodies the values of the age in which it was created. When the atomic bomb was being developed in the mid-nineteen-forties, the destruction of cities and the deliberate

targeting of civilians was just another military tactic. It was championed as a means to victory. The Geneva Conventions later classified those practices as war crimes—and yet nuclear weapons have no other real use. They threaten and endanger noncombatants for the sake of deterrence. Conventional weapons can now be employed to destroy every kind of military target, and twenty-first-century warfare puts an emphasis on precision strikes, cyberweapons, and minimizing civilian casualties. As a technology, nuclear weapons have become obsolete. What worries me most isn't the possibility of a cyberattack, a technical glitch, or a misunderstanding starting a nuclear war sometime next week. My greatest concern is the lack of public awareness about this existential threat, the absence of a vigorous public debate about the nuclear-war plans of Russia and the United States, the silent consent to the roughly fifteen thousand nuclear weapons in the world. These machines have been carefully and ingeniously designed to kill us. Complacency increases the odds that, some day, they will. The "Titanic Effect" is a term used by software designers to explain how things can quietly go wrong in a complex technological system: the safer you assume the system to be, the more dangerous it is becoming.