R. JAMES WOOLSEY
TESTIMONY
BEFORE THE
HOUSE COMMITTEE ON ENERGY AND COMMERCE
May 21, 2013

This hearing is about cyber threats and solutions. But I am going to talk about a dimension of the cyber threat that is not usually considered a cyber threat in Western doctrine, but is in the playbooks for an Information Warfare Operation of Russia, China, North Korea, and Iran. These potential adversaries in their military doctrines include as a dimension of cyber warfare a wide spectrum of operations beyond computer viruses, including sabotage and kinetic attacks, up to and including nuclear electromagnetic pulse (EMP) attack.

It is vitally important that we understand that a nuclear EMP attack is part of cyber and information warfare operations as conceived by our potential adversaries. Our cyber doctrine must be designed to deter and defeat the cyber doctrines of our potential adversaries by anticipating how they plan to attack us--but our doctrine currently does not.

Our cyber and information warfare doctrines are dangerously blind to the likelihood that a potential adversary making an all-out information warfare campaign designed to cripple U.S. critical infrastructures would include an EMP attack.

The assessment that nuclear EMP attack is included in the cyber and information warfare doctrine of potential adversaries, and the effects of an EMP attack described here, are based on the work of the Congressional EMP Commission that analyzed this threat for nearly a decade (2001-2008). The Congressional Strategic Posture Commission and several other major U.S. Government studies independently arrived at similar conclusions, and represent collectively a scientific and strategic consensus that nuclear EMP attack upon the United States is an existential threat.

What is EMP? A nuclear weapon detonated at high-altitude, above 30 kilometers, will generate an electromagnetic pulse that can be likened to a super-energetic radio wave, more powerful than lightning, that can destroy and disrupt electronics across a broad geographic area, from the line of sight from the high-altitude detonation to the horizon.

For example, a nuclear weapon detonated at an altitude of 30 kilometers would project an EMP field with a radius on the ground of about 600 kilometers, that could cover all the New England States, New York and Pennsylvania, damaging electronics across this entire region, including electronics on aircraft flying across the region at the time of the EMP attack. The EMP attack would blackout at least the regional electric grid, and probably the entire Eastern Grid that generates 70 percent of U.S. electricity, for a protracted period of weeks, months, possibly years. The blackout and EMP damage beyond the electric grid in other systems would collapse all the other critical infrastructures--communications, transportation, banking and finance, food and water--that sustain modern civilization and the lives of millions.

Such an EMP attack, a nuclear detonation over the U.S. East Coast at an altitude of 30 kilometers, could be achieved by lofting the warhead with a meteorological balloon.

A more ambitious EMP attack could use a freighter to launch a medium-range missile from the Gulf of Mexico, to detonate a nuclear warhead over the geographic center of the United States at an altitude of 400 kilometers. The EMP field would extend to a radius of 2,200 kilometers on the ground, covering all of the contiguous 48 United States, causing a nationwide blackout and collapse of the critical infrastructures everywhere. All of this would result from the high-altitude detonation of a single nuclear warhead.

The Congressional EMP Commission warned that Iran appears to have practiced exactly this scenario. Iran has demonstrated the capability to launch a ballistic missile from a vessel at sea. Iran has also several times practiced and demonstrated the capability to detonate a warhead on its medium-range Shahab III ballistic missile at the high-altitudes necessary for an EMP attack on the entire United States. The Shahab III is a mobile missile, a characteristic that makes it more suitable for launching from the hold of a freighter. Launching an EMP attack from a ship off the U.S. coast could enable the aggressor to remain anonymous and unidentified, and so escape U.S. retaliation.

The Congressional EMP Commission warned that Iran in military doctrinal writings explicitly describes making a nuclear EMP attack to eliminate the United States as an actor on the world stage as part of an Information Warfare Operation. For example, various Iranian doctrinal writings on information and cyber warfare make the following assertions:

- "Nuclear weapons...can be used to determine the outcome of a war...without inflicting serious human damage [by neutralizing] strategic and information networks."

- "Terrorist information warfare [includes]...using the technology of directed energy weapons (DEW) or electromagnetic pulse (EMP)."

- "...today when you disable a country's military high command through disruption of communications you will, in effect, disrupt all the affairs of that country....If the world's industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults, then they will disintegrate within a few years."

China's premier military textbook on information warfare, written by China's foremost expert on cyber and information warfare doctrine, makes unmistakably clear that China's version of an all-out Information Warfare Operation includes both computer viruses and nuclear EMP attack. According to People's Liberation Army textbook *World War, the Third World War--Total Information Warfare*, written by Shen Weiguang, "Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse...and quickly achieve breakthroughs in those technologies...":

> *With their massive destructiveness, long-range nuclear weapons have combined with highly sophisticated information technology and information warfare under nuclear deterrence....Information war and traditional war have one thing*

in common, namely that the country which possesses the critical weapons such as atomic bombs will have "first strike" and "second strike retaliation" capabilities ....As soon as its computer networks come under attack and are destroyed, the country will slip into a state of paralysis and the lives of its people will ground to a halt. Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse...and quickly achieve breakthroughs in those technologies in order to equip China without delay with equivalent deterrence that will enable it to stand up to the military powers in the information age and neutralize and check the deterrence of Western powers, including the United States.

North Korea appears to be attempting to implement the information warfare doctrine described above by developing a long range missile capable of making a catastrophic nuclear EMP attack on the United States. In December 2012, North Korea demonstrated the capability to launch a satellite on a polar orbit circling the Earth at an altitude of 500 kilometers. An altitude of 500 kilometers would be ideal for making an EMP attack that places the field over the entire contiguous 48 United States, using an inaccurate satellite warhead for delivery, likely to miss its horizontal aimpoint over the geographic center of the U.S. by tens of kilometers. North Korea's satellite did not pass over the United States--but a slight adjustment in its trajectory would have flown it over or near the U.S. bull's eye for a high-altitude EMP burst.

North Korea appears to have borrowed from the Russians their idea for using a so-called Space Launch Vehicle to make a stealthy nuclear attack on the United States. During the Cold War, Moscow developed a secret weapon called a Fractional Orbital Bombardment System (FOBS) that looked like a Space Launch Vehicle, but was designed to launch a nuclear warhead southward, away from the United States initially, but deliver the warhead like a satellite on a south polar orbit, so the nuclear attack comes at the U.S. from the south. The United States has no Ballistic Missile Early Warning (BMEW) radars or missile interceptors facing south. We might not even see the attack coming.

Miroslav Gyurosi in *The Soviet Fractional Orbital Bombardment System* describes Moscow's development of the FOBS:

The Fractional Orbital Bombardment System (FOBS) as it was known in the West, was a Soviet innovation intended to exploit the limitations of U.S. BMEW radar coverage. The idea behind FOBS was that a large thermonuclear warhead would be inserted into a steeply inclined low altitude polar orbit, such that it would approach CONUS from any direction, but primarily from the southern hemisphere, and following a programmed braking maneuver, re-enter from a direction which was not covered by BMEW radars.

"The first warning the U.S. would have of such a strike in progress would be the EMP...," writes Gyurosi.

The trajectory of North Korea's satellite launch of December 12, 2012 looked very much like a Fractional Orbital Bombardment System for EMP attack. The missile launched southward, away

from the United States, sent the satellite over the south polar region, approaching the U.S. from the south, at the optimum altitude for EMP attack--although the test trajectory deliberately avoided flying over the United States.

North Korea appears to have borrowed from Russia more than the FOBS. In 2004, a delegation of Russian generals met with the Congressional EMP Commission to warn that design information for a Super-EMP nuclear warhead had leaked from Russia to North Korea, and that North Korea might be able to develop such a weapon "in a few years." A few years later, in 2006, North Korea conducted its first nuclear test, of a device having a very low yield, about 3 kilotons. All three North Korean nuclear tests have had similarly low yields. A Super-EMP warhead would have a low-yield, like the North Korean device, because it is not designed to create a big explosion, but to produce gamma rays, that generate the EMP effect.

According to several press reports, South Korean military intelligence concluded independently of the EMP Commission that Russian scientists are in North Korea helping develop a Super-EMP nuclear warhead. In 2012, a military commentator for the People's Republic of China stated that North Korea has Super-EMP nuclear warheads.

One design of a Super-EMP warhead would be a modified neutron bomb, more accurately an Enhanced Radiation Warhead (ERW) because it produces not only large amounts of neutrons but large amounts of gamma rays, that cause the EMP effect. One U.S. ERW warhead (the W-82) deployed in NATO during the Cold War weighed less than 50 kilograms. North Korea's so-called Space Launch Vehicle, which orbited a satellite weighing 100 kilograms, could deliver such a warhead against the U.S. mainland--or against any nation on Earth.

Iran may already have a FOBS capability, as it has successfully launched several satellites on polar orbits, assisted by North Korean missile technology and North Korean technicians. Iranian scientists were present at all three North Korean nuclear tests, according to press reports.

What is to be done about the Cyber and EMP threats?

Technically, it is important to understand that surge arrestors and other hardware designed to protect against EMP can also protect against the worst-case cyber scenarios that, for example, envision computer viruses collapsing the national power grid. For example, surge arrestors that protect Extra High Voltage transformers from EMP can also protect transformers from damaging electrical surges caused by a computer virus that manipulates the grid Supervisory Control And Data Acquisition Systems (SCADAS).

Administratively, a coherent and effective answer will not likely arise from uncoordinated decisions made independently by the thousands of individual industries at risk. Because cyber preparedness should encompass EMP preparedness--and since EMP is an existential threat--it is imperative that Government play a supervisory and coordinating role to achieve protection against these threats swiftly.