Rising Nuclear and Cyber threats require up gradation of Nuclear Command and Control Capabilities

The potential use of nuclear weapons poses the greatest danger to U.S. security. According to the U.S. National Security Strategy, Recently Nuclear threat is rising again due to nuclear arms race in asia, modernisation of nuclear arsenal by Major and regional powers, statement by countries like North Korea to use nuclear weapons, ongoing missile and nuclear proliferation risks in the Middle East and acquiring of Nuclear weapons by terrorists.

North Korea has said that says it is ready to use nuclear weapons against the United States and other foes if they pursue “their reckless hostile policy” toward Kim Jong Un’s regime and that Pyongyang is improving its nuclear weapons arsenal “in quality and quantity.” “If the U.S. and other hostile forces persistently seek their reckless hostile policy towards the DPRK and behave mischievously, the DPRK is fully ready to cope with them with nuclear weapons any time,” the director of the North Korean Atomic Energy Institute said.

“North Korea’s nuclear weapons program made remarkable progress in 2017, increasing risks to North Korea itself, other countries in the region, and the United States. Hyperbolic political rhetoric and provocative actions by both sides have increased the possibility of nuclear war by accident or miscalculation,” Rachel Bronson, the president of the Bulletin of the Atomic Scientists, said in a statement.

Al Qaeda and other Islamist terrorist groups have explored the possibility of acquiring nuclear weapons to be used against

their enemies. “The Islamic State has billions of dollars in the bank, so they call on their wilayah (province) in Pakistan to purchase a nuclear device through weapons dealers with links to corrupt officials in the region,” the article, attributed to British photojournalist John Cantlie held hostage by Islamic State for over two years, said. Once the Islamic State buys the bomb in Pakistan, according to the article, it would transport it through Libya and Nigeria to the West.

Nuclear Policy has also enhanced the risk as and both Pakistan and Russia incorporating the early use of nuclear weapons into their war-fighting plans. VLADIMIR Putin recently hit out at at America “and its allies” for plotting against Russia to neutralize its nuclear capabilities and insisted he would respond by developing weapons that would “penetrate any missile defence shield”. Mr Putin said: “References to Iran and North Korea nuclear threats are just a cover for the true purpose (of NATO missile defence).

Nuclear threat is also being enhanced by cyber warfare. CHERNOBYL nuclear power plant was suspended in June 2017 after being hit by ransomware cyber attack, which caused chaos across Europe. The rising cyber threat has put into question the survivability and reliability of Nuclear Command and Control from cyber attack and other accidents.

US is also considering nuclear response against cyber warfare against its critical infrastructure. According to the New York Times, The Trump administration plans to change its “Nuclear Posture Review” to allow the first use of nuclear weapons, in response to “attempts to destroy wide-reaching infrastructure, like a country’s power grid or communications, that would be most vulnerable to cyberweapons”. Countries are also contemplating cyber warfare against nuclear threats. It has also been reported that US has been contemplating a cyber attack, to disable an adversary’s nuclear capability.

Rising Nuclear threat due to Modernization and Expansion of Nuclear Capability

In response to Nuclear threats, All the Major Powers are upgrading and modernizing, all of the three legs of their strategic triad to provide a strong deterrent against perceived adversary threats.

The Obama administration had planned a three-decade-long plan costing more than $1 trillion, with $350 billion in the first decade alone. These include Ground-Based Strategic Deterrent, Next-Generation Bomber LRS-B and the new ballistic missile submarines, the SSBN(X). US president-elect Donald Trump twittered in late December that the United States “must greatly strengthen and expand its nuclear capability until such time as the world comes to its senses regarding nukes”. Later, he declared: “Let it be an arms race,” and asserted that the US would win it.

Russia planned to spend 101 billion rules on nuclear modernization program from 2013 to 2015, partly in response to the development of a global missile-defense system by the Americans. The current Russia NATO confrontation over Crimea, Ukraine or Baltic States is also driving it to spending billions of dollars on modernizing its strategic arsenal. These include Topol-M ICBMs, 5th generation submarines and PAK-DA a subsonic stealthy flying wing aircraft.

Nuclear Command and control safety and security

The rising Nuclear threat is further compounded by survivability and reliability of Nuclear Command and Control from cyber attack and other accidents. Command and control systems are the brains of the Nuclear Weapon Infrastructure which provide states to plan the management, deployment, and potential release of nuclear weapons. They allow military and political leaders to ensure with high confidence that the weapons will detonate when their use is ordered, but that they will not do so by accident or without authorization. PBS American Experience documentary suggests that it's a miracle that we all survived the Cold War. Not because of the Soviet threat, but because there was a good chance that the USA could've blown itself up with one of its own nuclear weapons.

Future nuclear missiles may be siloed but, unlike their predecessors, they'll exhibit "some level of connectivity to the rest of the warfighting system," according to Werner J.A. Dahm, the chair of the Air Force Scientific Advisory Board. "We have a number of nuclear systems that are in need of recapitalization," said Dahm, referring to LRSO, ICBMs and the B-21 stealth bomber. In the future, he said, "these systems are going to be quite different from the ones that they may replace. In particular, they will be much more like all systems today, network connected. However increased connectivity also pose nuclear threat because of increased vulnerability from cyber attacks from adversaries and terrorists..

"Nuclear weapons systems are designed so that several things would have to go wrong to result in an accidental or unauthorized missile launch or nuclear explosion. For most of the past incidents, only one or two things went wrong, so that in many cases the incident did not in itself pose a serious risk," says the report of union of concerned scientists,

“Close Calls with Nuclear Weapons”. However, these historical incidents show that system failures occur on a routine—even frequent—basis.

Such system failures reduce the number of effective safety measures in the system. System failures also make it more likely that under the time pressure and confusion of a crisis, or under an unexpected confluence of circumstances, safety measures will be eroded to the point that an unintended detonation or launch can occur.

Cyber threat to Nuclear command and Control

Franz-Stefan Gadysays in his article provides three War Games-like scenarios, “First, sophisticated attackers from cyberspace could spoof U.S. or Russian early warning networks into reporting that nuclear missiles have been launched, which would demand immediate retaliatory strikes according to both nations’ nuclear warfare doctrines. Second, online hackers could manipulate communication systems into issuing unauthorized launch orders to missile crews. Third and last, attackers could directly hack into missile command and control systems launching the weapon or dismantling it on site (a highly unlikely scenario).

“One-half of their [U.S. and Russian] strategic arsenals are continuously maintained on high alert. Hundreds of missiles carrying nearly 1,800 warheads are ready to fly at a moment’s notice,” a policy report compiled by a study group chaired by the retired U.S. general summarized.

The policy report further said, “At the brink of conflict, nuclear command and warning networks around the world may be besieged by electronic intruders whose onslaught degrades the coherence and rationality of nuclear decision-making.”

“De-alerting” nuclear arsenals could help reduce the likelihood of a cyberattack causing an accidental nuclear war between the United States and Russia, retired U.S. Gen. James Cartwright recently stated in an Associated Press interview.

The threat could also be minimized by up gradation of Nuclear command and control networks, making them hackproof to cyber attacks.

Nuclear command and control (NC2) is the activities, processes, and procedures performed by appropriate military commanders and support personnel that, through the chain of command, allow for senior-level decisions on nuclear weapons employment. Therefore there is urgent need for countries to modernize their Nuclear Command and Control Strategies, procedures and processes to make them hack proof as well as improve their quality.

Rockwell Collins enhancing E-4B Advanced Airborne Command Post

Rockwell Collins is upgrading the low-frequency transmission system of the US. Military’s E-4B Advanced Airborne Command Post.
“We’re continuing our strong relationship with Boeing by providing reliable, survivable and endurable communications between the President (of the United States) and our nation’s nuclear forces,” said Troy Brunk, vice president and general manager, Airborne Solutions for Rockwell Collins.

The E-4B Advanced Airborne Command Post is designed to be used by the National Command Authority as a survivable command post for control of U.S. forces in all levels of conflict, including nuclear war. It also supports the U.S. Federal

Emergency Management Agency by providing communications following natural disasters

Northrop Grumman up upgrade SATCOM capability for Navy E-6B airborne command post

Northrop Grumman Corp. will build and test advanced SATCOM capability involving the Multi-Role Tactical Common Data Link (MR-TCDL) for the U.S. Navy E-6B Mercury strategic airborne command post and communications relay aircraft under terms of an $12.2 million contract modification. MR-TCDL provides Ku line-of-sight and Ka SATCOM systems for the E6-B. The data link includes two Ku line-of-sight channels and one Ka satellite communications channel. Other equipment includes power conditioning, cooling, electrical, and network distribution.

The E-6B provides command and control of U.S. nuclear forces should ground-based control become inoperable. The plane is based on the four-engine Boeing 707 passenger jetliner.

Russia Upgrades Airborne Command Post

One of Russia’s four Ilyushin Il-80 airborne command posts has been modernized and has passed state acceptance trials.
Both the Il-80 and its larger American equivalent, the Boeing E-4B Advanced Airborne Command Post, are intended to control armed forces in the event of a nuclear war or of all-out conventional war with massive air strikes. The Il-80 carries senior commanders of the Russian armed forces, along with a team of officers from the general headquarters and a group of technical specialists to service the onboard equipment.

According to the United Instrument-building Corporation, the airplane's staff can execute control over the Land Forces, Navy, Air-and-Space Force and Strategic Missile Nuclear Force. The Il-80 can also be used during the overseas deployment of troops, or when ground-based control infrastructure is not available.

The Il-80 has a gross weight of 208 metric tons (457,000 pounds) and a maximum unrefueled range of 11,000 km (about 6,000 nm). Outwardly, the Il-80 differs from the baseline passenger jet in having a large satcom dome above the front fuselage; an in-flight refueling probe; and two 9.5-m (3 foot)-long underwing pods each carrying a turbine generator that feeds electrical power to onboard systems. There are only a few fuselage windows and hatches, so as to protect the equipment inside from the aftermath of a nuclear explosion.

The United Instrument-building Corporation further reports that it has already started work on a third-generation airborne command post. This effort is led by its member company NPP Polyet, based in Nizhny Novgorod

The article sources also include:

http://nationalinterest.org/blog/the-buzz/modern-command-control-critical-maintaining-us-nuclear-15918

https://www.theatlantic.com/technology/archive/2016/12/hacking-into-future-nuclear-weapons-the-us-militarys-next-worry/511904/

https://www.theatlantic.com/technology/archive/2016/12/hacking-into-future-nuclear-weapons-the-us-militarys-next-worry/511904/