Ploy and Malice - Attempts by Terrorist Movements to Acquire Non-Conventional Weapons

Dr. Ehab Khalifa

Researcher and Writer Specializing in Technology and Extremism Issues, Egypt

Given how difficult it is to obtain non-conventional weapons, particularly nuclear weapons due to the stringent security measures in the manufacturing, transport, and circulation of nuclear materials, it is still doubtful that terrorist organisations could do so. Assuming that terrorist organisations stole or otherwise acquired a nuclear weapon, its transfer and employment in terrorist operations would necessitate acts that terrorist organisations are unable to carry out, including acquiring ballistic missiles or enormous aircraft. However, this did not stop terrorist organisations from attempting. For example, in order to carry out an attack inside a nuclear reactor or steal nuclear materials, some broke into a nuclear facility in Brussels in 2016.

Drone Bombing

In September 2022, a book was published by Abu Muhammad al-Masri, a leader of al-Qaeda, entitled The 9/11 Operations: Between Truth and Uncertainty, in which he tackled the attempts of terrorist groups to carry out a nuclear explosion by directing a drone loaded with thousands of highly flammable fuel containers, to one of the nuclear reactors in the US. In view of the great development in cyber weapons in the past decade, and what can be done with them by penetrating nuclear facilities, or tampering with safety systems inside reactors, as happened at the Iranian Natanz nuclear facility in 2009, there has been increasing concerns about terrorist groups launching cyberattacks targeting nuclear reactors.

In his book, al-Masri listed unconventional ideas for carrying out a nuclear explosion, such as relying on members of Muslim communities and minorities working in nuclear facilities, and employing their resentment against the US because of its policies of racial discrimination, to recruit them to carry out attacks inside these facilities, or to carry out acts of sabotage that lead to radiation leakage to make some areas unfit for human life. In this regard, his book states that:

“the huge stockpile of nuclear weapons on US territory is a major vulnerability if militant groups can access it, and test part of it on US soil, making the US an uninhabitable land. This is not unlikely, but how to access this strategic stockpile needs to be studied thoroughly. .... The US military has operatives from the Muslim community, as well as Africans who feel humiliated by the non-stop actions of white supremacists, and by taking advantage of these charged souls we can reach the goal and benefit from a qualitative blow”.

This is purely theoretical, in addition to extremist groups’ actual attempts to carry out nuclear sabotage. For example, the Brussels bombings carried out by Daesh in March 2016, which revealed that the perpetrators of the operation planned to launch a nuclear attack by blowing up a nuclear plant, killing the guard of one of the facilities, and taking his access card to launch a bombing inside the facility. The police found a 12-hour video of surveillance depicting the home of one of the Belgian nuclear program managers, part of a plan to kidnap him and force him to let them into the nuclear facility.

Nuclear Cyberattacks

One of the threats posed by cyber weapons or computer viruses is their ability to target nuclear facilities. Although the nuclear cybersecurity of the facility is the most important element of safety and security, a study issued in 2016 within The Nuclear Threat Initiative showed that half of the countries with nuclear facilities in the world do not have legislation or procedures for cybersecurity to protect facilities from cyberattacks! This means that most of these facilities are susceptible to dangerous cyberattacks in varying degrees.

Managing to own one of these viruses, buy it over the Dark Web, leak it from some governments, or obtain it by recruiting professional hackers, terrorist groups can pose a real nuclear threat, which will in no way amount to a nuclear explosion due to safety and security measures inside these facilities, but may result in damage to devices and systems, and radiation leakage.

States are generally too sensible to launch cyberattacks that result in a nuclear catastrophe. However, terrorist groups, criminal organizations and extremists are not that reasonable. Some groups may be able to launch cyberattacks on and penetrate into a nuclear facility, leak important information about it, or change the reactor management system, leading to partial failure of the reactor or radiation leakage.

Nuclear facility operators and managers are aware of these threats, but the problem is that several traditional methods of cyber defense at nuclear facilities—firewalls, anti-virus technology, and air gaps that separate internal reactor networks from the internet—are no longer sufficient to keep up with escalating threats.

The Stuxnet worm is the first example of the use of a cyberweapon in targeting a nuclear reactor. It was used to target the Iranian nuclear program in 2009, and was considered one of the most dangerous types of cyber weapons. Ever since, the risk of cyberattacks that threaten nuclear facilities has increased.

In December 2014, the South Korea Hydro and Nuclear Power Corporation (KHNP) announced that its computer systems had been hacked, but only insignificant data was stolen. Authorities found evidence indicating the removal of a low-risk electronic worm from devices connected to some control systems at a nuclear-powered power plant, and accused North Korea of involvement in the attack. Also, in April 2016, malicious viruses were discovered on computers in the Gundremmingen reactor in Germany. They also hit 18 mobile media used to transmit data inside the reactor, but did not affect the work of the reactor because industrial processes are disconnected from the internet.

These previous examples emphasize the urgent need to reconsider cyber safety procedures at nuclear facilities, or else they will become vulnerable to threats. A strong terrorist group with a strong organization and leadership determined to achieve the goals could cause sabotage of some nuclear facilities that leads to dangerous radiation leakage.

Chemical and Biological Compounds

Chemical and biological weapons are less dangerous than nuclear weapons, but their use may result in a significant loss of life due to their ease of transport, such as unleashing a virus in a flowing river or releasing deadly chemical compounds and gases in one of the main squares, or in buses and trains.

Therefore, chemical and biological weapons have become an alternative to nuclear weapons for terrorist movements because of their easy access, installation, carrying, and deployment. The Organisation for the Prohibition of Chemical Weapons (OPCW) has monitored the use of mustard agent in an attack launched by terrorist Daesh in 2015 in northern Syria, which led to the injury of at least 20 people. The town of Marea, located near the Turkish border in Aleppo province, which was then under opposition control, was bombarded with munitions filled with chemicals believed to be mustard sulfur. A

New York Times report confirmed that Daesh used chemical weapons in Syria and Iraq more than 52 times between 2014 and 2016.

The German Criminal Police arrested two Daesh extremists, who were planning to launch a biological bomb attack in the country in June 2018. The indictment prepared by the Anti-Terrorism Prosecution stated that they decided in the fall of 2017 to launch an attack in Germany, and detonate an explosive device in a large crowd of people, to kill and injure as many people as possible.

Morocco announced the discovery of lethal bio-toxic substances in the possession of a Daesh terrorist cell arrested on February 18, 2016 in the city of El Jadida in central Morocco.

Morocco's Interior Ministry stated that Daesh's operatives in the Moroccan city of El Jadida prepared these deadly materials for use to implement their terrorist agenda inside Morocco.

Finally, we assert that the technological revolution and its smart ways have contributed to shifting power sources and methods of application. Online, information has become a major source of power, including information about vital facilities that may become the target of terrorist attacks, such as nuclear facilities, power plants, airports, and research laboratories, as well as information on how to make explosive devices, purchase explosive materials or conventional weapons, or create computer viruses to launch cyberattacks against nuclear power plants, biofuels, and critical state infrastructure.

This significant change in sources of power has enabled extremist terrorist movements to achieve goals that in the recent past were impossible for them. This technological development, just as it helped terrorist movements change their military plans in the past few years, may help them even more in the coming years, if we do not dry up their sources and combat their tools.