Vinci Nicolò 08/04/2021

**EXERCISE 4**

**Cyber attack in Venezuela:**

Personally, I think that the vulnerabilities exploited by the group of attackers are two: the lack of redudancy in the fiber optic network and a poor access control due to the partecipation of foreign agents.

First of all, the access control system should be stronger in order to avoid the access of foreign agents and even the access in the fiber optic network by the attackers. Besides, the Movilnet’s GSM should have predicted some backup links for the connectivity of the country. In this way the mobile phone service would still be active even if the nine cuts.

To sum up, the Movilnet’s GSM should have decreased substantially the likelihood of this attack applying a stricter access control system. Therefore, they would still have ensured the connectivity of the country after the attack thanks to backup links, so the impact would have been less.

**“Lights Out!” Did Trump and His Neocons Recycle Bush Era Plan to Knock Out Venezuela’s Power Grid?:**

The Venezuela’s power grid is knocked out by the Nitro Zeus cyber attack. It is a dreadful attack which was born to mitigate the Stuxnet worm. The Nitro Zeus aims to make unavailable the communications, power grid and other vital systems that are necessary resources even for the population.

It is very difficult to state some preventive controls given that the Nitro Zeus seems so powerful that it can pass any access control mechanism and make unavailable any backup or auxiliary systems. The common preventive controls such as a stricter access control service or auxiliary power grid may not work. However, the auxiliary power grid may be placed in a safe place so that the Nitro Zeus can not discover it. Anyway, a better solution would be to isolate the attacked infrastructures and try to make a sort of reverse engineering to discover more information on Nitro Zeus. This way may be useful to understand which vulnerabilities are exploited, but the Nitro Zeus may be so sofisticated to not leave traces of itself.

There are not enough information to understand which preventive controls may be effectively useful against the Nitro Zeus. A massive reverse engineering analysis may lead to know more details on it.