The problem outlined by the two articles is very vast, has deep political implications and probably a solution, if it exists, it may be only partial. The following paragraphs attempt to provide at least some preventive controls on the matter (seen from Venezuela’s point of view) to avoid similar situations in the future.

To begin with, the current geopolitical situation must be taken into account. The U.S., a first world superpower (at least for now), has contingency plans for every possible country and every possible disaster people can think of. No way any other country or any other person will be able to convince them to drop any plan, even their biggest allies. This is just part of being proactive in case of any disaster or any war. This is true both for war plans and cyber security plans. In the future, attacks will surely (and mostly already have) become more and more network-oriented and less physical oriented (i.e. less bombs and more malware). Either way, people will still continue to play a critical role in any attack whatsoever: this includes planting moles, counterspying, social engineering, etc… Everything must be taken into account, but nothing can be truly stopped given the circumstances.

In 2021, I believe it is now customary even for lesser developed countries to begin fostering development of network security agencies, invest in cybercrime prevention, and in general be prepared for the cyberwarfare that will be common in the years that follow. One might argue that countries such as Venezuela might have other business in their heads, and rightfully so, given the situation. However, at least some measures could be taken in order to provide a basic level of security that Venezuela might have been lacking at the time.

This bullet list provides a general idea of what could be implemented by Venezuela, in the form of preventive fixes regarding three separated areas that were targeted by the attack plus some general suggestions.

GENERAL PREVENTIVE CONTROLS

* border controls (to prevent moles, undercover agents, etc…)
* creation/strengthening of counterspying agencies, in order to be more proactive in case any other country may want to replicate this attack
* strengthening of cyber security response and prevention teams (as stated above)

POWER GRID

* thorough checkup of electronic systems, to verify installation of unauthorized equipment or malfunctions
* renovation of outdated systems that may be sensible to hijacking

OPTIC FIBER

* introduction of redundancy / alternative routes: if a route is cut off then traffic can be temporarily diverted to it without much disruption
* better security in network hotspots, by using guards and access control systems

MOBILE NETWORK

* better network segmentation, so that outages or attacks in a zone do not affect other ones
* adoption of newer technologies (GSM is insecure, 3G won’t hold longer)
* physical access controls (as above, using guards) in areas with antennas / cells

In conclusion, while risk is always present and must be accepted in some form, some countermeasures could be taken (and should have been taken), that could have at least mitigated the immense outages suffered by Venezuela in 2017.