

Ground Truth: Attack on Electric Grid and Banking System.

Infrastructure Category: Energy, Information Technology, Financial Services

Threat Details: The hacking group OCR (Original Constitution Republic) has attacked the electrical grid in California and Texas, causing widespread regional outages. They also attacked a couple of regional banks and destroyed the IT assets of the banks. They used social media to create panic and fuel protests of the American people. They also encouraged local militias to restore law and order in America because the current government is not capable.

Origin of the threat: A new hacking group calling themselves OCR has formed. Their belief is that the US government and corporations are corrupt and need to change. They support the original intent of the Constitution and the first ten amendments. They believe that all federal agencies are unconstitutional and should be disbanded. They believe that the US should not be involved in any foreign affairs and focus on helping Americans first. They believe the border should be militarized, only landowners can vote, and that power should return to the States. They have recruited domestic militia groups with similar views and told them to be ready to act.

Other Impacting Factors: OCR uses Social Media disinformation to sway public opinion in their favor. Their hacking skills and disinformation campaign skills suggest foreign government support. OCR is suspected of being supported by Russian, Chinese, and North Korean hackers.

Unfolding response: Federal and State governments have to respond to regional power outages, a run on the banks, violent protests, and militia groups taking the law into their own hands. This is complicated by certain politicians supporting OCR and the militias in an election year. This political support lends legitimacy to their views, and a small vocal group of voters support OCR's positions and methods.