Saudi Arabian Policy on Cyber Capabilities

By Brian Curnett
Under the Guidance of Dr. Samuel Liles

Summary
Saudi Arabian policy replaces cyber security with cyber censorship which led to the vulnerabilities which exposed the nation’s oil industry to attack. As a compensatory mechanism, foreign nation’s contractors were hired to solve technical problems rather than developing a domestic knowledge base. This has made the nation of Saudi Arabia more vulnerable for the long term.

Saudi Policies continue this cycle by simply patching problems and never looking toward the long term with reinvestment in its people.

Companies such as IBM are brought in to create regional security operation centers.

CITC/KACST: Saudi government agency responsible for maintaining a nationwide firewall on “objectionable material. Due to funds expended on censorship Saudi belief is that cyber security has been funded. This perception leaves the nation vulnerable.

Attacks like the Shamoon Virus upon Saudi Aramco on the critical national infrastructure.