CERIAS

The Center for Education and Research in Information Assurance and Security

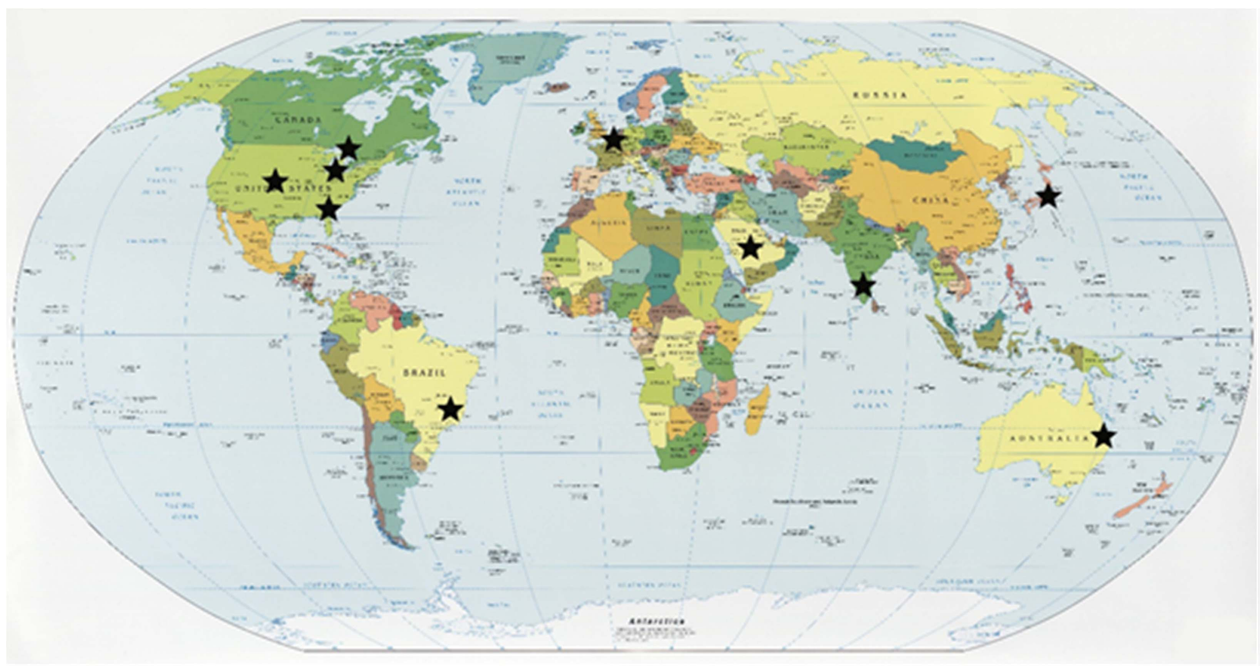
Saudi Arabian Policy on Cyber Capabilities

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 then nation's oil industry to attack. As a compensatory mechanism foreign nation's contractors 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.



Cultural Bias

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.

Censorship

Lack of Protection

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

Contracted Solutions

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

Misplaced Policies

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