Study advised US on Libya hacking

June 13 2011, By RAPHAEL G. SATTER , Associated Press

(AP) -- Private computer experts advised U.S. officials on how cyberattacks could damage Libya's oil and gas infrastructure and rob Moammar Gadhafi's regime of crucial oil revenue, according to a study obtained by hackers.

It remains unclear who commissioned "Project Cyber Dawn" and how much of a role the U.S. government played in it, but it shows the increasing amount of work being done by private companies in exposing foreign governments' vulnerabilities to cyber attack.

"For the private sector to be making recommendations ... that's a level of ambition that you would not have seen until very recently," said Eli Jellenc, a cyber security expert with VeriSign Inc. who is not linked to the study or its authors.

The study outlined ways to disable the coastal refinery at Ras Lanouf using a computer virus similar to the Stuxnet worm that led to a breakdown in Iran's enrichment program late last year. It catalogued several pieces of potentially exposed computer hardware used at the refinery.

The study was discussed in some of nearly 1,000 emails stolen by hacking group Lulz Security from Delaware-based Internet surveillance firm Unveillance, LLC as part of an effort to show how vulnerable data can be. Most of the emails detail the day-to-day trivia of running a small technology startup, but others concern an effort to scout out vulnerabilities in Gadhafi's electronic infrastructure.

Cyberwarfare has assumed an increasingly high profile following dramatic computer attacks on Google, Inc., U.S. defense contractors and the IMF. This month, the Pentagon is expected to release policy on whether some cyber attacks should be considered acts of war and when a U.S. cyber attack might be justified.

Project Cyber Dawn was put together by the Cyber Security Forum Initiative, a group whose membership includes military officials, academics and business leaders. Unveillance Chief Executive Karim Hijazi was one of the report's 21 co-authors, among them forum founder Paul de Souza and Jeffrey Bardin, a former NSA code breaker.

The group posted a redacted version of the study online on May 25, around the time that Hijazi realized his emails had been compromised, but by then the unredacted version was already online.

Bardin declined to answer specific questions about the unredacted version of the study. He acknowledged in a blog that it was circulated to "defense and intel types" but he refused to go into any further detail when contacted by email, saying only that he and his colleagues "are proud of the work we did."

Through a representative, Hijazi referred questions about the report to de Souza, who in a statement said it was aimed at "educating the international community" about the risks of an attack on the industrial control systems at oil refineries in Libya.

But the recommendations are apparently addressed to American officials and contain suggestions on how U.S. intelligence could best spy on the current or any future Libyan administration. Despite repeated emails, de Souza did not clarify how such advice would be useful to an international audience.

The authors of Cyber Dawn argued that something similar to the Stuxnet attack on Iran could be done in Libya, noting that German engineering conglomerate Siemens AG - whose software system was exploited by Stuxnet - has played an important role in projects across the North African country.

At Ras Lanouf, which has the capacity to handle 220,000 barrels of oil per day, the report identified the computers involved in running the refinery's power plant as vulnerable because some were the same Siemens-brand hardware as the kind used in Iran. A Germany-based spokesman for Siemens didn't return an email seeking comment.

Ras Lanouf remains under Gadhafi's control, and, as the Libyan civil war drags on, governments might see a cyberattack on such a facility as a discreet and bloodless way of cutting into Gadhafi's oil revenue.

It remains unclear who was briefed about Cyber Dawn, and whether any of its ideas were taken onboard.

Several of the leaked emails suggest that the report was circulated among Pentagon officials, presidential staffers, and a group at the ODNI, presumably the Office of the Director of National Intelligence.

"Our final report will make it to the White House," Bardin wrote in one of the emails.

But senior defense officials told The Associated Press they were unaware of the study. Officials, speaking on condition of anonymity because they were not authorized to describe internal discussions, said the Department of Defense gets unsolicited reports all the time, and that some of them may be reviewed by staff.

U.S. government cybersecurity experts would not comment on what, if

any, hacking operations are being waged against the Gadhafi regime.

More information:
Officially released version of Project Cyber Dawn: http://ow.ly/5bSIj (.pdf)

Bardin's explanation of Cyber Dawn: http://ow.ly/5cPOO

Unveillance statement on the hack: http://ow.ly/5cPMJ

Cyber Security Forum Initiative: http://www.csfi.us/