High-tech weapons sow fears of chip sabotage

April 17 2011, by Dan De Luce

A Libyan rebel stands near a rocket launcher in the western gate of Ajdabiya. As NATO countries weigh whether to arm Libya's rebels, military planners may give a thought to adding a remote "kill switch" to some weapons to keep them out of the wrong hands, experts say.

As NATO countries weigh whether to arm Libya's rebels, military planners may give a thought to adding a remote "kill switch" to some weapons to keep them out of the wrong hands, experts say.

Even if allied governments conclude that building in a remote control to disable anti-tank launchers might be more trouble than it's worth, the mere possibility is transforming the role of high-tech weapons in warfare.

"The more advanced technology becomes, the more it becomes

integrated in networks, the more opportunities there are for attacks," David Lindahl, a research scientist at the Swedish Defence Research Agency, told AFP.

The growing sophistication of modern weaponry, with its reliance on electronic circuits and robotics, has fueled speculation that the United States or other powers might choose to turn off their weapons remotely -- or secretly sabotage the enemy's high-tech systems.

The original version of a "kill switch" dates back to the peak of the Cold War, when permissive action link (PAL) devices were introduced in the 1960s to prevent a rogue launch of a nuclear missile.

But Lindahl and other technology specialists say there is no evidence that the United States or other countries use remote "kill switches" in other weapons.

Designing a remotely controlled switch would be a costly, complicated undertaking, and few defense companies would be enthusiastic about inserting a vulnerable link into one of their products, experts said.

If Western countries chose to retrofit anti-tank missiles for Libya's rebels with "kill switches," they would still face the risk that adversaries might eventually get a hold of the weapons and uncover design secrets, Lindahl said.

"It's incredibly risky to do something like that," he said.

As chip manufacturing has migrated outside the United states, American defense officials have long worried about foreign countries finding a "backdoor" into the Pentagon's sensitive weapons systems.

"There are two ways to look at this. You build them into your own

weapons, or the second way is you unwittingly incorporate them into your own weapons because someone sold you a bad chip," said James Lewis, a cyber expert at the Brookings Institution think-tank and former US official.

To guard against possible sabotage, the Pentagon has tried to ensure a secure supply of microchips by certifying some fabrication plants in the United States, known as the Trusted Foundries Program.

But defense manufacturers, no longer able to avoid using commercial off-the-shelf products, face growing risks to their supply chain and software, experts said.

"The military systems nowadays are not purpose-built from scratch. You have soft systems surrounding them," Lindahl said.

Fears that foreign-made chips could contain secret codes that would allow an adversary to disable or seize control of a weapon may be overstated, said Lewis.

"It's something you have to be concerned about, that you have to think about when you build the weapon, but it's harder to do than it looks," Lewis said.

He added that "concerns about supply chain can easily shade into paranoia." Technology bloggers and experts have long speculated that Israel may have manipulated Syria's radar when it bombed a nuclear facility in 2007.

Syria's high-tech air defenses should have detected the Israeli jets but bloggers say the country's radar -- using off-the-shelf chips -- may have contained tainted processors with secret "backdoors," allowing Israel to somehow disable or deceive the radar.

The strike on Syria illustrates how sometimes just the idea of a dangerous microchip is just as effective as the genuine article.

"If there is a kill switch, it makes sense the Israelis would use it. If it doesn't have a kill switch, it makes sense they would spread the rumor," Lindahl said.

(c) 2011 AFP