ALJAZEERA

Cyber warfare: Where are the limits?

We examine how far the US itself is pioneering offensive cyber policy.

March 29, 2013

A NATO-commissioned report suggests an alleged US cyber attack on Iran's uranium enrichment programme was an "act of force" that was likely illegal. And Microsoft with Google admitted it allowed the FBI to spy on its customers.

Stuxnet was a computer worm discovered in June 2010 that was allegedly created by the US and Israel to target Iran's nuclear facilities.

However, the US has never owned up to involvement.

Now a 300-page manual commissioned by NATO and written by legal scholars and military lawyers from member countries suggests the attack was an act of force prohibited under the United Nations charter.

After months of the US national security establishment sounding the alarm on the need to defend against potential cyber threats, questions are again being raised about how far the US itself is pioneering offensive cyber policy.

Domestically, American privacy campaigners have been reacting to an admission from Microsoft that the FBI has been able to access customer data by issuing what are known as national security letters that do not require a judge's approval.

So was the Stuxnet attack an illegal act of force? Are the US offensive cyber policies crossing the limits? And are the private rights of the American citizens at risk?

To discuss this, Inside Story Americas is joined by guests: David Kravets from Wired magazine; Alfredo Lopez, an internet freedom activist; and Julian Sanchez, a research fellow at the Cato Insitute who focuses on technology and civil liberties.

"Certainly there is an act of force, and their policy does seem to leave it open, that if they considered it equivalently damaging to a physical attack that a military response might be justified, so this is the principle they are applying. And in a way it makes a certain ammount of common sense, you don't want to say that taking down an airplane with a stinger missile is an act of war but doing it with a laptop isn't. There is a lot of complications in cyber aspects that make it more dangerous and difficult to apply those rules clearly. It seems like in this case there is the classic attribution problem with cyber attacks, that is, unlike a missile being launched it's much more difficult to know within a great certainty where an attack really originated from."

- Julian Sanchez, a research fellow at Cato Institute