**Crossing the Line: When Cyberattacks Become Acts of War**

There is a silver lining between pulling pranks and committing criminal offense.The biggest question when does the attacker crosses the line and it converts into cyber war.  Cybersecurity professionals never do such attacks however the role of cyber security professionals is to defend the IT sector by reducing the risks and keeping the things running smoothly. Cybercriminals are always behind one’s money and data, but our role is to protect common man from such criminals and minimise the damage when they do it.

What is act of war

As per oxford dictionary, “*An act of war by one nation intended to initiate or provoke a war with another nation; an act considered sufficient cause for war*.” Infecting a virus in country’s industries can cause a lot of havoc. A lot of examples stands like *SolarWinds breach* that was found in December. One more example like *Stuxnet worm* which was a decade ago. Both the incidents became major incidents with political and diplomatic repercussions, but never turned into a war.

When it crosses the line?

It crosses ever limit when the cyber attacks causes major loss to county’s infrastructure. The whole world is connected in modern times and due to advancement in technology the threats have become more dangerous and vulnerable, and maybe can cross the line. Civilians do not have legal permission do commit such crimes. There’s a Cold War of sorts going on in cyberspace. Paying techniques might have changed and targets have grown in numbers. Still it haven’t crossed the limit yet.

As cybersecurity professionals, it’s our job to secure our organisations against these attacks. If we educate the common people then we can prevent cyber attacks and if these attacks happens then we will be in a position to come out of the situation.

Thank you