Why you should see the ZERO DAYS documentary…

It’s “WORLD WAR 3.0” and the stakes have never been higher.

The Internet – and devices that connect to it – is the battleground.

…Other countries hack our industrial, military and technology secrets.

…Organized crime steals and sells our personal and corporate financial info and holds critical computer networks hostage for ransom.

…Outside activists infiltrate government, business and organizations, stealing policy docs and private communications.

…Hackers for hire do all of the above plus orchestrate public opinion in our country to benefit outside interests.

…Most of the major players have the ability to shut down power grids, transportation systems, water supplies, financial, defense and security networks, etc.

…Our country has a publicized defensive capability and an offensive capacity that, by necessity, is far less visible.

In 2007, three years before the StuxNet virus destroyed Iran’s nuclear centrifuges, the Idaho National Laboratory ran the **Aurora Generator Test** to demonstrate how a cyberattack could destroy physical components of the electric grid. The experiment used a computer program to rapidly open and close a diesel generator's circuit breakers out of phase from the rest of the grid and cause it to explode. This vulnerability is referred to as the *Aurora Vulnerability*.

In 2009, The United States created the **Cyber Command** **(CYBERCOM)** subordinate to US Strategic Command, at the National Security Agency (NSA) headquarters in Fort Meade, Maryland. It uses NSA networks and has been headed by the Director of the NSA since its inception. While originally created with a defensive mission in mind, it is increasingly viewed as an offensive force.

According to its mission statement, CYBERCOM is empowered to “conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.”