Norwegian cyber defence force

Parts of the World, Europe

Although the vast cyberspace development amongst nations in recent years has led to an improvement in the many fields of communications, it has been recognised that governments, terrorist organisations and activist groups have resorted to misuse these developments for their own purposes. Governments use cyber technology to their advantage by spying on classified activities, nuclear developments and secret negotiations between other governments to foresee harmful actions that may disrupt peace times. Meanwhile for terrorist organisations and hacktivist groups, cyber technology is used to create anarchy and to cause disputes between governments that may lead to cyber warfare. Cyber warfare has become a method for individuals/groups to unidentifiably hack, obtain and leak sensitive and classified information without creating an act of war. Due to cyber technology’s evolution, the anonymity given to hackers spying and revealing data has created many rivalries between countries, causing them to oppose each other and further improve their ability to spy for security purposes. It appears that after the introduction of nuclear bombs in the arms race, cyber warfare, although it seems more subtle, it can create more social, political and economical havoc and chaos. Hence, cyber espionage has transformed the world and has brought about a new era of warfare, one that is difficult to predict, detect and trace, often leading to conflicts between countries uninvolved.

As a nation, Norway has tremendous potential in cyberspace. Norway heavily relies on its ‘ Norwegian Cyber Defence Force (NCDF)’; an extremely well developed force that has the potential to protect data, carboy attacks and espionage attempts. Norway believes that in this age of cyber warfare, no country, organisation or individual should have the sovereignty to spy and leak sensitive information of private firms, public data or military developments. It is in this policy that Norway proposes to direct the committee in a direction wherein laws on cyber technology is made stricter and more efficient ways of ensuring that these laws aren't broken.

The first draft solution presented by Norway is that, a separate UN framework must be formed, which will have access to all parliamentary data of governments to ensure no illegal/secretive actions are taking place such as negotiations with terrorist organisations, spying on individuals or mass production of nuclear weapons. This frameworks purpose is more or less to monitor information of governments to ensure no government can use cyber espionage on citizens of its own country or other governments. If this framework acknowledges an act of aggression being performed by a nation, the act shall be notified to the UNGA an the aggressor shall be condemned.

By monitoring all governments like this, the need for organisations such as 5 eyes or espionage becomes redundant as any provoking act taken by a nation shall be alerted to other countries. Another solution Norway proposes is that if countries agree to create a framework as listed above and adhere to it then the countries must also abolish the groups they have created to share specific intel. Through this, global tensions between countries of opposing blocs can be consoled as the formation of blocs itself begins to dissolve, making nations neutral in cyber warfare or cyber espionage. Thirdly, Norway proposes that the member nations of DISEC can use their existing espionage technology and developments to tackling rogue, hacktivist, anarchist organisations such as Anonymous and LulzSec to prevent social and political upheavals in the future as the sole purpose of such organisations is to spread anarchy and dissolve governments.