Noé Kurata

Tek01 IT, Epitech 06/12/2022

**How are countries adapting to cyber warfare?**

Did you know that wars aren’t only consisted of physical violence between two countries? It can also be a group of people or country attacking another through attacks via the internet. Nowadays everyone uses internet and has a life on the internet whether it is through social media, video games, websites, etc. Most people’s and governments data are saved to the internet (aka: the cloud = networked computing facilities providing remote data storage and processing services via the internet). In this essay we are going to talk about cyber warfare and how countries are adapting to cyberwarfare. First, we will define cyberwarfare, in a second part we will see why we will engage in cyberwarfare. Finally, we will see how we can avoid cyberwarfare.

Cyber ​​warfare is defined as an electronic attack against computer systems to use them as a means of propaganda and disinformation, or to cripple the vital activities of a country. Since the creation of the Internet, the global network has become a place of military conflict. The use of the Internet makes it possible to infiltrate the most sensitive networks, but this has created a movement where the targets are now government sites of institutions, large and medium-sized enterprises, those of private organizations and individuals. These attacks are often carried out by groups of hackers who are people who, for fun, challenge, or seeks for a profit or looking to circumvent the protections of software, to fraudulently enter a system or a computer network. These hackers are instrumentalized by states or political or religious groups to carry out attacks and participate in cyber warfare.

Cyber warfare can be started by anyone; but why would someone trigger a cyberattack? The only reason for launching cyberattacks are either to recover or destroy data or to practice espionage. Data is an element that serves as a basis for reasoning, a starting point for research. Confidential data is often targeted by these attacks, the loss or theft of which could harm the strategic interests, the security or the very existence of a company. Espionage constitutes a crime, an attack on the fundamental interests of the nation accomplished by someone for the benefit of a foreign nation. This is generally used to collect data on the person / group targeted or to disseminate data or false information to influence the crowds.

Now that we have defined what cyber warfare is, given the reasons for cyberwarfare and cyberattacks and that we have seen how countries protect themselves from these cyberattacks, we can ask ourselves the following question, how can cyberwarfare be avoided?

In 2010 the United States created the USCYBERCOM which is part of the United States Law Enforcement which is used to launch cyberattacks against threats in the United States and serves to defend against these attacks. In 2017 France decided to create its own Cyber ​​Defense Command (COMCYBER) which is placed under the authority of the Chief of Defense Staff, and which fulfills the same functions. In addition, there is more and more security coming out in the private sector to secure access to the internet and to secure our data like VPNs. A VPN, or virtual private network, is a service that encrypts your activity on the internet and keeps your identity hidden while navigating the internet. VPN technology was first used in 1996 when a Microsoft employee developed the PPTP. All of this allow countries and large companies to avoid suffering or countering cyberattacks and if there are no counterattacks, cyberwarfare can be avoided.

In conclusion we can say that cyberwarfare already exists with moments of different intensities (currently more intense in parallel with the armed conflict in Ukraine) and that a solution to maintain cyberwarfare in its state of threat is similar to that on nuclear power which is to make sure to find a balance between the forces of the different belligerents to avoid massive attacks that would find equally massive counterattacks as a response.