Cyber Warfare And Espionage: Country Stance And Solutions

Constant technological development in the 21st century has brought about new national security concerns for many countries, with cyber warfare and espionage becoming extremely common. Recent attacks on the US election, Estonia and other countries have highlighted this growing problem. Cyber espionage being covert and completely untraceable has encouraged many countries to survey and gain information from other countries. This information can then be used to cause political damage like the US elections, economic damage like that in Estonia, or even physical military damage such as the stuxnet virus deployed in Iran. We've seen cyber-attacks move from enthusiasts to financial thieves to now governments around the world.

Alarmingly however has been the increase in cyber-attacks by non-state actors and terrorist groups. With cyber-attacks requiring less capital, people and military might, this is proving to be an effective way for terrorist organizations to wreak havoc in the modern world. Despite some countries boasting a very large cyber defense squad, virtually every country is susceptible to a cyber-attack. Furthermore organizations like ISIS use media to post gruesome images of killing in order to spread fear among the world. Moreover they use the dark web to secretly recruit people for their organization. The primary problem with cyber warfare is its vagueness. Firstly the never ending cyberspace poses problems for any government due to its vastness. The definition of cyber warfare and cyber espionage is not yet universally agreed upon and this hence creates problems for countries when determining the severity of an attack and its consequences.

Countries build their cyber-attack arsenal in the name of peace and security and then end up using this on smaller or more vulnerable nations to disrupt that peace. Larger countries such as USA and Russia have done this on numerous occasions thereby breaking their allies trust. An example of this is the Edward Snowden leaks that revealed the extent to USA’s spying on neighboring and allied countries. This created a sense of distrust for the USA; however more importantly highlighted the imminent danger of these attacks. Countries now have to live in fear and hope that they are not attacked. This situation can cause disharmony between many previously allied countries. Overall Cyber-crime is a problem that could result in chaos and destruction unless prevented. Ironically man’s biggest accomplishment of the 21st century, the internet, may now prove to be its biggest weakness.

COUNTRY STANCE

Slovenia is a country that believes in freedom of its people and hence doesn't impose any harsh internet regulations. With more than 6 times as many cyber- attacks than in 2008 Slovenia recognizes the growing need of a well-developed cyber security network to prevent attacks by regular hackers, states or non-state groups. Slovenia has recently developed and been part of many organizations to spread awareness and to find solutions to this problem. As a less powerful country we are concerned of our lack of preparedness if any powerful cyber-attack were to occur on our economy. We believe in alliances and support from larger countries such as the USA and agree that to solve these problem first concrete definitions need to be set out. Our limited resources however are preventing us from rapid progress in this field hence we encourage the UN to find a solution. We condemn Russia for its attacks on the less powerful and are wary of the development of the Baltic States.

SOLUTIONS

1. Increased awareness for people of the country - The people of our country are not entirely aware of the dangers of cyberspace and cybercrime. Give importance to SI-CERT's educational program "Safe on the Internet". Have similar campaigns on cyber security. Encourage programs such as The SAFE.SI program that operates as a national point for raising awareness among children and adolescents about the safe use of the Internet and mobile devices.
2. Create a unilateral definition of cybercrime, cyber warfare and cyber espionage. Clearly differentiate between what actions can be classified as espionage and what actions can be classified as cyber warfare in order to remove and vagueness and then implement regulations for these actions. Decide upon the punishment and penalties for breaches of cyber space, cyber espionage and cyber warfare respectively. These punishments can possibly be sanctions on trade or large fines to the victim country in order to rebuild their economy. Countries that have already committed cyber-attacks should also be punished for their actions. A body can be created to decide and oversee these punishments. This group relates to paragraphs 9, 41 and 42 of UN resolution 65/230.
3. Setting up organizations to provide funding and resources for the research and development of cyber defenses to the smaller countries to combat cybercrime. State based attacks such as those in Estonia or Iran should be condemned and should never be allowed happen to any "smaller" country.
4. Increase the fourteen eyes alliance to include many other NATO countries like Slovenia. Maybe use this formed alliance can be used to collectively combat terrorism and other action groups with the intention of inflicting harm or chaos upon a country or its people.