Cybersecurity policies and solutions in yemen

Science, Computer Science

As times progress, a new manmade dimension, cyberspace, has emerged, which poses the problem of cyber espionage and cyber warfare. In today's day and age, the entire world is dependent on the internet and technology, which has improved significantly, which would lead to one thinking that a nation's security has increased. However, this development in technology has caused it to become easier than ever to attack a country's entire communication system and to suspend cyber activity, which essentially controls all technological and electrical activity, of vast regions.

Causes

Since cybercrime is a relatively new form of attack, laws to prevent it have a certain ambiguity to them and the cybersecurity of certain nations is not up to mark. Due to this and the fact that the cost required to perform cyber warfare is low as compared to the cost of its alternative, i. e. a war, hackers and government organisations have seen this as a better option of offense. Tracing a cybercrime is also extremely difficult which leads to hackers believing that they can get away with it. Hence, due to low probability of getting caught, low severity of punishments if found guilty, and high ambiguity of laws according to which a hacker is prosecuted, cybercrime is seen as the favourable method of attack.

Current state of problem

Cyber-attacks can be divided into three parts, i. e. Computer Network Exploitation (targeting computer networks to extract and collect data), Computer Network Attack (damaging of other networks) and Computer Network Defence (cybersecurity). Due to the cyberspace being so vast, unknown and connected, it has become easier to penetrate devices set up to ensure cyber security, but it has become harder to figure out the culprit behind these attacks. A lack of proper legislation with respect to this topic has also caused an increase in cybercrime. Popular methods of cybercrime include phishing, Denial of Service attacks, Snake virus and Sandworm virus. Russia, China and North Korea are generally suspected to be guilty when a cybercrime takes place with respect to hacking of government websites. However, due to the aforementioned difficulty to prove one guilty in such a scenario, little action has been taken against these countries. The Five Eyes organisation is a popular alliance between USA, UK, Canada, Australia and New Zealand that maintains a policy of sharing of information about other governments and such acquired through cyber-attacks.

Policies

Yemen currently does not have any laws to prevent crime in this field. With a civil war raging in the country, cyber security is important but, however, not one of the main priorities of the government. However, there is a draft legislation concerning this area of crime which will be put in action as soon as possible. With cybercrime having become part of this war, it is more necessary than ever to impose laws to prevent and reduce this. It is imperative for the government of Yemen to regain control of the internet from the Houthis. Cybercrime committed by rebels against the government has increased the need to improve cyber security. The Houthis have cut off internet supply for around 80% of the nation. They have also shut down the internet for a certain period of time. This has shone light on the fact that although it is not a main priority, it is still extremely important and necessary for the government to improve our cyber security. However, this is not their first cyber-attack. Previously, the Yemen Cyber Army, consisting of rebels, attacked a Saudi website and leaked information. Seeing their misuse of power and attack on our ally, the government feels that cyber laws need to be imposed immediately to combat the rebels' cyber-attacks.

Solutions:

1) Urges all underdeveloped nations to improve their cybersecurity by:

a) Seeking help in training of IT professionals from the UN

b) Approaching previously trained IT professionals, unemployed at that moment, to join these agencies of their country

c) Asking their allies for economic resources to improve one's cybersecurity;

2) Encourages all advanced and developed nations to:

a) Improve cybersecurity due to a higher probability of their governments being hacked and cybercrime becoming an increasingly popular method of attack

b) Join the aforementioned training programme which would be applicable to all nations

c) Provide economic help to underdeveloped allies when approached to provide better cybersecurity

3) Proposes an improvement in the legislation of various countries by:

a) Defining cybercrime, cyber-attack, cyber espionage and cyber warfare and these definitions must be universally accepted

b) Increasing the severity of the punishment issued to a cyber criminal, i) Thus, with a low probability of getting caught and with a low probability of being punished, even in which case the punishments would not be too severe, cyber criminals find cybercrime to be a safer route of attack, ii) However, if the chances of being punished if found guilty are increased, along with the severity of the punishment, cybercrime could be greatly reduced

c) Reducing the ambiguity of the laws with the help of the new definitions and increasing severity of the punishment in countries with existing laws

d) Introducing new laws, in countries with either no laws or extremely few laws that don’t cover the topic to an adequate extent, in accordance to the newly created definitions and ensuring that an adequate punishment should be served if these laws are not followed.

Conclusion

This ever-growing problem of cyber-attacks can be combatted by implementing various laws, increasing the severity of the punishment if caught, and most importantly increasing cyber security. With a better understanding of various concepts relating to cybercrime and increased control of cyberspace, cyber-attacks can be combatted.