Assignment 2: Chanakya Gaur

Review national cybersecurity strategies of select countries(Canada)

This summary is based on “*Canada’s Cyber Security Strategy. For a Stronger and More Prosperous Canada*” published in 2010. Canada defines cyberspace as a world created by interconnected networks of information technology and the information on those networks. It is a global common where more than 1.7 billion people are linked together to exchange ideas, services and friendship and defines cyber security as Cyber-attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber-attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security. [1] Canada has had its fair share of cyber-attacks with McMaster University reporting a study that 51.7 million Canadians were victims of identity theft in 2008 leading to a loss of approximately $2 billion. Canadian companies also reported that 86% of the large companies suffered a cyber-attack. Owing to the rise in cyber-crimes, Canada amended its cyber policy to include identity theft and reduce cybercrime. According to Canada, most cyber-attacks share similar characteristics which account for their growing popularity: they are inexpensive, easy, low risk and effective.

To mitigate these threats, Canada’s Cyberspace Security Policy is built on three pillars: Securing Government Systems, partnering to secure vital cyber systems outside the Federal Government and helping Canadians to be secure online. Canada secures its government systems by using the necessary tools, structures and personnel. Canada partners with provincial and territorial governments along with the private sector to initiate steps to strengthen security including critical infrastructure protection. The government also asks input from various stake holders to increase resiliency. Canada has established some specific initiatives for this purpose.

Canada established clear federal roles and responsibilities. It assigned Public Safety Canada to coordinate the implementation of strategy. Public Safety Canada is also the central organization to asses emerging complex threats and come up with ways to address them. The Communications Security Establishment has the role to deal with detecting and discovering new threats, provide foreign intelligence and respond to any attack against the government network. The Canadian Security Intelligence Service analyzes domestic and international threats to the security of Canada. The role of Foreign Affairs is to advise on the international aspect of cyber security. Using such resources helps Canada to ensure that they constantly strengthen their security. The government also has taken initiatives to educate people to be safer and aware. Canada also partners with its allies to exchange information and be safer together.

Canada has a clear and defined policy which mainly stresses on three things. Firstly, Canada believes that the country can be safe from attacks only if al agencies work together and contribute. Which is why Canada is having multiple organizations contributing in the space of cybersecurity. Secondly, Canada also makes sure that it educates its citizen to be aware. A line from their policy states that they aim to educate citizens to not assume that their systems are safer than they actually are. This reflects upon the preventive caution Canada is trying to instill in their citizens. Thirdly, Canada is making sure that they have multinational communication to make sure they are updated upon the latest threat and can mitigate them in time. However, the educative points mention in the policy seem a bit outdated even if they are valid and I feel that they should be updated.