The New Geopolitics of Cybersecurity

Name

Institutional Affiliation

Cybersecurity is increasingly becoming a high-profile field. New risks attached to the same continue to escalate as governments are playing foreign politics using security companies (Bambenek, 2018). Over the past years, cyber operations have turned to a significant point for regional conflict and a major source for power competition. State-based hackers have identified crucial infrastructure, held that information, accessed personal data, as well as state secrets. Further, they continue to interfere with the democratic system using disinformation campaigns. The international regulations that govern these actions have proven unable to keep pace with these aspects and the danger to international stability is significantly heightened (Bambenek, 2018).

Consequently, the continued technology advancement has not made it easier as it continues to change strategic elements such as artificial intelligence and quantum information science. Today, in the United States, cybersecurity has become one of the daily aspects the government seeks to address. For instance, the House voted to restore State cyber officer. President Donald Trump termed cybersecurity as a national defence priority (Bambenek, 2018). The two aspects are a clear indication of how it is of paramount importance to address issues of cybersecurity as they make a nation vulnerable to attacks that could result in huge damages. Further, the United States as one of the measures has employed the sanction program as a way of fighting overseas cyber attackers (Bambeneck, 2018).

Besides, there are recent events that have emerged as a result of geopolitics cybersecurity. One of them is the 2016 elections (Bambenek, 2018). The fact that the United States 2016 election was under cybersecurity threat can only mean that the world is facing a Cold War of cyber espionage and the repercussions amounting from the same continues to escalate. In this election, it is believed that data was hacked from the Democratic National Committee Server to enable the direct influence of the election itself. Russia was the source of the attack. The sought of the attack has a danger in that it changes the whole essence of an election process. Secondly, the WannaCry and NotPetya were primary reasons as to why people got turned away from hospitals in 2017. The ransomware initially put a claim as a warning from the FBI in demanding a fine, by putting threats to users to pay up and posing blackmails on them. The other observed event was the Olympic destroyer (Bambenek, 2018). The 2018 Olympics were the most deceptive cyberattack of history. The attacker had manipulated his way into the RFID systems and knew perfectly that the opening ceremony would have ended within a short while and the athletes, dignitaries and spectators would discover they had no WI-FI connection as well as access to the Olympics app.

In relation to the above, it clear that nations are under more visibility than they have ever been in the past. Cybersecurity officers are getting fired as a result of breaches (Bambenek, 2018). The political world is becoming a perception as the world is liberated from all these aspects, as what was previously held as private Intel is now leaked to press (Bambenek, 2018). Failure to evaluate information adequately is costing the organization a lot as compared to when the same could have gotten the necessary attention. There exist official and non-official cover spies. Kaspersky Software is what the Russian government is using as a spy tool. The Russian government uses the tool to search for the United States classified information (Bambenek, 2018). Russian’s have threatened to pose a retaliation if the members of Pentagon banns Kaspersky Software. Banning the same would prove challenging as the tool is mostly significant amongst firms. The tool allows organizations to collect client telemetries, exchange information with law enforcement, protect against threats such as APTs, as well as research on new threats.

In conclusion, there has emerged a third class of spy with no cover. When one of these individuals get picked for spying, the only thing the government does is to find a list of lawyers for them and let the family know they will be home late. Thus, what one country perceives as legal, could be termed illegal in another country. Many foreign government target individuals working in security research as they are seen as spies (Bambenek, 2018). The more cybersecurity has turned out as a political aspect, the more political governing comes into play. Hence, the same translates into perception management. When cybersecurity becomes increasingly geopolitical, the more the concept becomes subject to laws of governments across the world. Hence, at times, research needs to be foregone when the risks in question are too high (Bambenek, 2018).

Reference

Bambenek. J. (2018, April 25). The New Geopolitics of Cybersecurity [Video] Youtube:<https://www.youtube.com/watch?v=RGkeQMJhQhE&authuser=0>