Russia's Foiled Cyber Attack on OPCW

Kritika Roy

Kritika Roy is a Research Analyst at the IDSA's Cyber Security Centre of Excellence.

Summary

Earlier this year, the Dutch Security services along with the help of British officials were able to thwart the plan of group of Russians to compromise and disrupt systems at the OPCW (Organisation for the Prohibition of Chemical Weapons). Russia's actions has brought to the forefront the grave reality of cyber threat that international organisations face today.

Russia's mushrooming cyber capabilities is well evident in the series of cyber activities that it has been undertaking lately. The country has been blamed for directing a host of cyber-attacks majorly to undermine western democracies by sowing seeds of confusion in everything from the 2016 presidential elections to the Global Chemical Weapons Watchdog. Earlier this year, the Dutch Security services along with the help of British officials were able to thwart the plan of group of Russians to compromise and disrupt systems at the OPCW (Organisation for the Prohibition of Chemical Weapons).

The OPCW is the implementing body for the Chemical Weapons convention. The OPCW with its member states has been instrumental in overseeing the global endeavor to permanently and verifiably eliminate Chemical weapons. Russia's actions has brought to the forefront the grave reality of cyber threat that international organisations face today. Attack on OPCW is actually a wakeup call for authorities to take stringent actions against states found involved in such activities.

The Motive

The OPCW attack comes at a time when the organisation has been probing the poisoning of a former Russian spy Sergei Skripal and his daughter Yulin Skripal. Their poisoning has said to be caused by using a toxic military grade nerve agent called the Novichok. (Novichok was developed during the cold War and is known as the fourth generation chemical weapon. This nerve agent is said to be more toxic than Sarin and even harder to identify.[1] Once exposed to this nerve agent, the victim could experience pupil constriction, continuous convulsions and vomiting, which could lead to fatal outcomes

like death or coma). Sergei Skripal was convicted in Russia of spying for Britain before he was granted refuge in the UK after a high-profile spy swap in 2010 between the US and Russia.[2] The nerve Agent used for poisoning him and his daughter was brought to the Cathedral City of Salisbury by two Russians who claimed to be tourists. However, the British official's investigations found them to be Russian agents.[3]

Contrarily, Russians had also requested the British government to allow their participation in the investigation of Skripal's poisoning. This request has fallen into deaf ears and therefore, Russia believes that such allegations are politically motivated campaign by the west and its allies to berate Russia. Apparently, the announcement of alleged Russian attack came just hours after the British National Cyber Security Centre connected six cyber international attacks to the GRU. These allegations included the meandering of 2016 US Presidential election and an attempt to infiltrate the World Anti-Doping Agency's Networks. As a part of growing efforts by the Western allies, they have started "naming and shaming" GRU and Russia for its alleged cyber activities.[4]

Another reason for targeting OPCW is said to be the organisations investigation of the alleged chemical attack in Douma by Syria's Russian backed military.[5] Being the top watchdog of chemical weapons, OPCW has allocated itself new set of responsibilities i.e. assigning blame for attacks. This move was protested by Russia. Russia tagged OPCW as a "sinking ship" and asserted that the organization was going beyond its mandate.

The Plot and the Suspects

Many reports suggests that proper planning and implementation was undertaken for the aforementioned cyber attack by Russia. The spying equipment's and the means of attack speaks volume of the preparedness and research the suspects had put into. According to military intelligence agency of Netherlands', four Russians were caught with spying equipment in the car park of a hotel nearby the OPCW headquarters in The Hague. They were reportedly trying to get into the computer network of OPCW. The plan was to compromise and disrupt the computers in the building by attacking the Wi-Fi networks. This means of attack is also known as "drive-by" attacks often waged to penetrate a target by harbouring hardware weak links. These weak spots of the hardware can be exploited to grab traffic.[6] There were also reports that "close access" teams to disrupt the systems were sent as the previous mechanism of sending "spear phishing" emails to the OPCW headquarters failed to work in the envisaged manner.[7]

The identified suspects were linked to the Russian military intelligence unit called GRU which has often been accused of conducting cyber operations. Two of the suspects, named Yevgeny Serebriakov and Alexei Morenets, were supposedly the cyber-operators. While the other two, named Alexei Minin and Oleg Sotnikov, were the support providers of the operation.

Conclusion

Despite all states have agreed that the international laws and norms of responsible state behaviour are encapsulating the cyberspace as well. Russia has continued its suspected activities in the cyberspace. In April 2018, the National Cyber Security Centre (NCSC) of UK, the Federal Bureau of Investigation (FBI) and the US Department of Homeland Security issued a joint alert about Russian cyber activity aimed at both the public sector, infrastructure and internet service providers (ISP).[8] Russians have refuted all the allegations by labeling them as "diabolical perfume cocktail" meant to

denigrate the Russian position in the international community.

There is no denying the fact that cyber attacks are a staunch reality in the Twenty-First Century. Waging cyber attacks gives nation states a strategic and asymmetric advantage as attribution and back tracing has always been a problem in investigating cyber attacks. However, targeting global organisations could actually raise several questions on safety and security of these organisation. Additionally, if these activities are gone unpunished then it could also give leeway to other rogue nations to undertake such initiatives in the foreseeable future, thus, undermining the international law and stability. It is high time that an example needs to be set such that a fear of consequence is instilled among the member nations. It is important to strengthen the resilience of the international institutions in the digital domain to restore faith in global organisations.

Endnotes:

1. Amesbury poisoning: What are Novichok agents and what do they do?" BBC, July 5 2018, see https://www.bbc.com/news/world-europe-43377698 accessed on 25 October, 2018.
2. Nathan Hodge, Emma Burrows and Tara John, "Putin: Sergei Skripal is a scumbag and traitor who betrayed Russia," CNN, see https://edition.cnn.com/2018/10/03/europe/putin-calls-skripal-scumbag-intl/index.html accessed on 25 October, 2018.
3. Kim Sengupta, "Russian spy agency GRU responsible for international cyberwar, UK government says," Independent, October 4, 2018, see https://www.independent.co.uk/news/world/europe/russia-gru-sergei-skripal-hacking-cyber-war-donald-trump-elections-a8567356.html accessed on 25 October, 2018.
4. David Bond, George Parker and Mehreen Khan, "Netherlands 'foils Russian cyber attack' on chemical weapons watchdog," The Irish Times, October 4, 2018, see https://www.irishtimes.com/news/world/europe/netherlands-foils-russian-cyber-attack-on-chemical-weapons-watchdog-1.3651549
5. "How the Dutch foiled Russian 'cyber-attack' on OPCW" BBC, October 4, 2018, see https://www.bbc.com/news/world-europe-45747472 accessed on 25 October, 2018.
6. Ibid.
7. "Russian cyber attacks are actions of 'pariah state', says UK," The Irish Times, October 5 2018, see https://www.irishtimes.com/news/world/europe/russian-cyber-attacks-are-actions-of-pariah-state-says-uk-1.3652662
8. n. 2.