Hacking has been defined as “intentional, unauthorized access to computer systems” (Potasznik, Day 12). Although hacking started as a joyous, “show-boaty” type of activity, it has become a very serious issue in the modern world. So much personal, private, and important information can be found on devices nowadays and this shift towards a technology centered society places all of this information at risk of being hacked. Malicious hacking is a very real issue globally, especially when it occurs between governments. Governments need to stay constantly on their toes when it comes to staying ahead of and dealing with “black hat” hackers from hostile countries. The latest instance of Russian hackers hacking Western governments and organizations via an existing Iranian spying operation that they hijacked demonstrates the need for governments to stay alert for hacking threats from all over.

Hacking is a global issue that many governments take seriously. The US, for instance has strict anti-hacking law in place: the Computer Fraud and Abuse Act of 1984. This law makes it illegal to access a computer without authorization, and results in either a misdemeanor or a felony charge depending on the cost it takes to fix any damages resulting from the hack (Potasznik, Day 12). Even though the US has this stringent law in effect against hacking, it is one of many countries that uses hacking to keep an eye on foreign adversaries. The National Security Agency (NSA), for instance, which was established in the US during World War II to decode messages, exists today with the sole purpose of spying on foreign entities (Potasznik, Day 5). This spying sometimes takes the form of hacking other governments or persons that appear to demonstrate malicious intentions towards the US. The NSA’s job is to ensure that the US remains safe from such foreign threats.
The most recent example of this type of threat comes from Russia and accidentally Iran. Russian hackers were able to launch dozens of cyberattacks on governments and organizations, including the US and Great Britain, while placing the blame on Iran, by taking control of an existing Iranian hacking infrastructure (Stubbs & Bing, 2019). Turla, the Russian group, utilized these Iranian tools to complete successful hacks into numerous organizations around the globe for a year and a half (Stubbs & Bing, 2019). The success of this group raises the question of how effective the US and other western governments are at truly protecting themselves from foreign hackers.

The discovery of these Russian hacks has certainly made Western governments more wary of the increasing sophistication and creativity of hostile hackers. This is seemingly the first instance of one state-backed hacking group masking their identity by hacking into a different hacking group. The US and Britain, in response to these hacks, have called for more awareness in governments when it comes to hacking activity. They make it a point to highlight their abilities to see beyond the masquerade and correctly identify the “cyber actors,” suggesting that they will continue to be successful at uncovering such deceptions (Stubbs & Bing, 2019). This situation obviously demonstrates the need of governments to stay alert when it comes to hacking so that such instances can be discovered and shut down rapidly.

Although I find it hypocritical of the US and Great Britain to call for more hacking awareness and shout out their own abilities to identify hackers (because both countries definitely have used hacking in the same way to spy on foreign hostile countries), I do agree that governments need to be more aware of the lengths hackers will go to in order to cause damage. Considering how much sensitive security and defense information exists on hackable devices, it is clearly important for governments to remain constantly vigilant against cyber attacks. When governments allow themselves to fall victim to hackers, they put the lives of millions at risk,
which should never be the case. This situation with the Russian hackers highlights the seriousness of this pervasive hacking situation that global entities now have to face on a daily basis.

References

