2024

Contrast and compare the cyber hacking laws between the United States, Russian federation, and the people's Republic of China

Kehinde Alabi
kalabi@my.harrisburgu.edu

CONTRAST AND COMPARE THE CYBER HACKING LAWS BETWEEN THE UNITED STATES, RUSSIAN FEDERATION, AND THE PEOPLES REPUBLIC OF CHINA

Alabi Kehinde Oluwasemilore

Information Systems Engineering and Management, Harrisburg University

CISSC 661: Principles of Cybersecurity & Cyberwarfare

Dr. Bruce Young

03/28/2023

Cybercrime as a rising issue

Cyber hacking is a growing threat in the modern world. As the world becomes more digital, the threat of cybercrime continues to grow. Cyberattacks can lead to stolen personal information, financial losses and damage to critical information. The increase in the digital transformation of companies has also led to an increase in cyber security concerns. With cybercriminals using increasingly advanced methods to gain access and take advantage of sensitive information. As a result, governments around the world have developed measures, laws, and regulations to address cybercrime and protect against cyberattacks. The United States, Russian Federation, and the People's Republic of China are among the countries with the most developed cyber hacking laws.

Cyber Hacking laws

Cyber hacking laws and regulations vary notably between the United States, Russian Federation, and the People's Republic of China. While all three countries have laws and regulations in place to address cybercrime, there are significant differences in their approach to cybercrime and their enforcement procedures.

United States

The United States has a long history of addressing cybercrime through laws and regulations. Cybercrime is mainly addressed through a variety of federal and state laws, including the Computer Fraud and Abuse Act (CFAA), which makes it illegal to gain access to computer systems without proper authorization. The CFAA laws also forbids interference of electronic communications, and the theft or destruction of digital information. In addition to the CFAA, the United States has several other laws and regulations put in place to address

cybercrime, including Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA).

The U.S. government has also created several agencies assigned to investigate and prosecute cybercrime including the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the Department of Justice (DOJ). In recent years, the U.S. has also taken an aggressive stance towards foreign cyberthreats including the establishment of the Cybersecurity and Infrastructure Security Agency (CISA) and the issuance of several executive orders to address cyber threats.

According to a joint statement from the Department of Homeland Security and Office of the Director of National Intelligence in October 2016, the United States accused Russia of hacking political organizations involved in the U.S elections and leaking pilfered information to influence the outcome. President Obama implemented sanctions in response to the hacking incident in December which negatively impacted his reputation in cybersecurity. The “hack and leak” campaign was specifically aimed at undermining American democracy which was in direct conflict with his administration’s efforts to promote democracy in the digital realm. This operation posed challenges for his emphasis on international laws and norms as the foundation for cybersecurity and exposed flaws in his attempts to prioritize deterrence as a crucial element of U.S. cybersecurity strategy (White House, 2016).

Russia

The Russian Federation has a criminal code that criminalizes cybercrime. The law prohibits unauthorized access to computer systems as well as the distribution of malicious software and cyber espionage. However, some critics have claimed that the Russian government has used its cybercrime laws to target political opponents. In addition, Russia has been accused

of being a haven for cybercriminals with some experts alleging that the government turns a blind eye to hackers operating within its borders if they do not target Russian interest. This has led to worries about the state's ability and willingness to effectively fight cybercrime. Furthermore, some critics argue that the laws are too broad and vague leading to the potential for abuse and arbitrary enforcement. In 2014, there was an attempt by the Russian business community to modify the country's security approach. They proposed the development of a national cybersecurity strategy which would involve the participation of businesses and civil society in the creation of cybersecurity standards and policy. The proposed strategy also aimed to increase international cooperation in cybersecurity and incorporate the experience of other countries (Chislova & Sokolova, 2021, p.246).

Towards the end of 2020, a new provision was added to the Russian Code of Administrative Offenses which established legal liability for non-compliance with regulations aimed at limiting access to information deemed illegal in Russia. Following this development, Roskomnadzor, the Russian federal executive body responsible for overseeing the media and telecommunications, issued orders to Facebook, Instagram, Twitter, TikTok, and several other online platforms to remove content related to unauthorized public protests. In response, investigations were launched, resulting in fines being imposed on some of the platforms for their failure to remove the targeted content. Non-compliance with Roskomnadzor's directive could lead to relevant platform being blocked or access to it being restricted in Russia, including limiting its loading speed.

Russia has been constantly accused of engaging in state-sponsored cyberattacks against other countries. The Russian government has been accused of orchestrating the 2016 hack of the Democratic National Committee in the United States, which was intended to influence the

outcome of the U.S. presidential election (CNN, 2018). The Russian government has denied involvement in the hack, but the incident has further strained relations between the two countries. Overall, the cyber hacking laws in Russia remain a complex and controversial issue with concerns about government surveillance, censorship, and abuse of power. While there are legal provisions in place to address cybercrime, their effectiveness and impartiality have been questioned. The international community has also raised concerns about the Russian government's alleged involvement in state-sponsored cyberattacks, which have the potential to destabilize global security and diplomatic relations.

China

As the world's second-largest economy, China holds a prominent position in the global cyber community due to having the highest number of internet users. With nearly 22% of the world's total users, China surpasses the combined numbers of the United States, India, and Japan. In comparison, the United States, with over a quarter-billion internet users as of 2017, ranks third in the world, behind China and India. Therefore, analyzing the cybersecurity policies and strategies of China and the United States can provide valuable insights into cybersecurity regulations worldwide. Given the importance of cybersecurity in economic development and international cooperation, identifying flaws in these policies is essential. The Chinese perspective on cybersecurity and terrorism sheds lights on their views, revealing that the country's unwavering support for cyber sovereignty suggests no change in its stance. Consequently, the People's Republic of China will probably continue to enhance its cyber capabilities for economic and national security purposes (Swaine, 2013).

In China, cybercrime is addressed through several laws and regulations, including the Cybersecurity law, the criminal law, and the National Intelligence Law. These laws are put in place by the government to cyber hacking and the dissemination of malicious software. However, the Chinese government has been criticized for theft of intellectual property and trade secrets from foreign companies. The Chinese government has also been accused of using its cyber capabilities to censor the internet and monitor dissidents. In, conclusion, China's cyber hacking laws are complex and multifaceted. As China continues to grow in influence on the global stage, its approach to cyber governance will likely have significant implications for the future of the internet and online freedom all around the world.

References

Chislova, O., & Sokolova, M. (2021). Cybersecurity in Russia. International Cybersecurity Law Review.

https://doi.org/10.1365/s43439-021-00032-9

Executive Order-Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities. (2016, December 29)

https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/executive-order-taking-additional-steps-address-national-emergency

Swaine, M.D. (2012). Chinese views on cybersecurity in foreign relations. China Leadership Monitor, (42).

https://carnegieendowment.org/files/CLM42MS_092013Carnegie.pdf

Chow, D. (2012). Doing business in China: Cases and materials.