SRMUN ATLANTA 2018

Our Responsibility: Facilitating Social Development through Global Engagement and Collaboration

November 15 - 17, 2018

sc_atlanta@srmun.org

Security Council Update No. 2: Threat of Cyber-attacks

Introduction

As technology and one's access to information continues to advance, new and evolving security risks and situations which threaten global peace and stability are generated. The reach of the internet extends transnationally to many facets of the public and private sphere which can be vulnerable to manipulation, theft, and hacking.[1] Nearly half the world, around 3.5 billion people, now have access to the internet and according to estimates by the Global Cybersecurity Index report of 2017, by 2020, there could be 12 billion machine-to-machine devices which are connected to the internet.[2] Not only is the public vulnerable to cyber-attacks, but private companies and government infrastructures have proven to have gaps in cyber security as well.[3] Both businesses and consumers are being overwhelmed by Ransomware cyber-attacks, incurring a high cost as attackers continue to demand higher ransoms.[4]

According to the Global Security Index, only 38 percent of Member States publish strategies for cybersecurity and approximately 12 percent of nations are in the process of developing cyber security strategies.[5] This means nearly half of all Member States are completely vulnerable to cyber-attacks and cyber terrorism.[6] According to the International Telecommunication Union (ITU), in 2016, tens of thousands of machines and electronics were targeted by cyber-attacks.[7] Additionally, as reported by the Global Cybersecurity Index in 2017, one in every 131 emails being sent was sent maliciously, which is the highest rate in the last five years.[8] This is why it is becoming increasingly important that Member States prioritize cyber security to combat the vulnerabilities of current cyber security infrastructure, raise awareness, and expand efforts to prevent future attacks.[9]

Human rights, as well as democratic processes and institutions, are being frequently threatened by cyber-attacks committed by authoritarian regimes and non-state actors.[10] These actors interfere with democratic processes by purposefully creating and spreading misinformation to influence voters, interfering with the voting process, altering voting results, and undermining citizen's confidence in trust in their democracy.[11] Cyber-attacks continue to threaten governments, political parties, and banks by freezing access to necessary data which halts business and government activity until the data can be accessed again. [12]

---

[1] "Democracy and cybersecurity" Ted Piccone, https://www.brookings.edu/wp-content/uploads/2017/08/fp_20170905_democracy_cyber_security.pdf (accessed September 15, 2018).

[2] "Global Security Index" International Telecommunication Union https://www.scribd.com/document/352985247/UN-report#fullscreen&from_embed (accessed September 15, 2018).

[3] "Global Security Index" International Telecommunication Union (accessed September 15, 2018).

[4] "Global Security Index" International Telecommunication Union, (accessed September 15, 2018).

[5] "Half of all countries aware but lacking national plan on cybersecurity, UN agency reports" UN News, https://news.un.org/en/story/2017/07/560922-half-all-countries-aware-lacking-national-plan-cybersecurity-un-agency-reports (accessed September 15, 2018).

[6] "Half of all countries aware but lacking national plan on cybersecurity, UN agency reports" UN News, (accessed September 15, 2018).

[7] "Half of all countries aware but lacking national plan on cybersecurity, UN agency reports" UN News, (accessed September 15, 2018).

[8] "Global Security Index" International Telecommunicaon Union https://www.scribd.com/document/352985247/UN-report#fullscreen&from_embed (accessed September 15, 2018)

[9] "Security Council Calls on Member States to Address Threats against Critical Infrastructure, Unanimously Adopting Resolution 2341" United Nations https://www.un.org/press/en/2017/sc12714.doc.htm (accessed September 15, 2018)

[10] "Democracy and cybersecurity" Ted Piccone, (accessed September 15, 2018).

[11] "Democracy and cybersecurity" Ted Piccone, (accessed September 15, 2018).

[12] "What Are the Most Common Cyberattacks" Cisco, https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html (accessed October 11, 2018).

More broadly, cyber-attacks threaten human rights. According to the United Nations General Assembly and the United Nations Human Rights Council, human rights as established by Universal Declaration of Human Rights should be protected equally on and off the internet.[13] This means that the public is protected from invasion of privacy and from mass surveillance as well as from cyber-attacks which may threaten the preservation of these rights.[14] Private citizens are often feel the burden of cyber-attacks, regardless of whether they were the intended target.

Recent Attacks

One of the most recent and widespread cyber-attacks was the WannaCry ransom attacks of 2017 in which 150 Member States were targeted, including the United Kingdom (U.K.), the Russian Federation (Russia), and the United States (U.S.).[15] The WannaCry worm is a type of Windows ransomware which encrypts files on individual systems via a security loophole in Windows operating system.[16] The WannaCry attacks targeted banks, hospitals, and organizations all over the world, demanding hundreds of dollars in digital currency to decrypt these important files.[17] Affected Member States have accused the Lazarus Group, a group with strong ties to North Korea, of being the perpetrators of the attack.[18] In a detailed report conducted by the Department of Health and Social Care (DHS) in the UK, they concluded that the lack of preparedness for such an attack coupled with the lack of communication between the government, health agencies, and businesses further exacerbated the effects of the attack.[19] In response, the UK has developed policies and response plans, particularly tailored to alleviate attacks in the healthcare industry.[20] The United Nations has since urged Member States to develop response plans to better handle cyber-attacks. [21]

In June 2017, Ukraine experienced a major cyber-attack, now referred to as NotPetya, where malware was released and quickly spread beyond Ukrainian boarders to the U.S., Russia, and Australia, among others.[22] This malware completely erased entire data centers bringing multiple companies' business activities to a halt.[23] Affected businesses included FedEx and Maersk which reported over USD 10 billion in lost profits, collectively.[24] While the Ukraine and U.S. have blamed Russia for the attacks, Russia has denied involvement. [25]Outside of accusations, there has been little international response to this attack.[26]

Cyber-attacks have also targeted governments and democratic institutions, as was the case with cyber-attacks during the United States' Presidential election in 2016. On June 14th, 2016, there was a cyber-attack launched against the

---

[13] "Democracy and cybersecurity" Ted Piccone, https://www.brookings.edu/wp-content/uploads/2017/08/fp_20170905_democracy_cyber_security.pdf (accessed September 15, 2018).

[14]"Democracy and cybersecurity" Ted Piccone, (accessed September 15, 2018).

[15] "In wake of 'WannaCry' attacks, UN cybersecurity expert discusses Internet safety" UN News, https://news.un.org/en/story/2017/05/557712-wake-wannacry-attacks-un-cybersecurity-expert-discusses-internet-safety (accessed September 30, 2018).

[16] "In wake of 'WannaCry' attacks, UN cybersecurity expert discusses Internet safety" UN News, https://news.un.org/en/story/2017/05/557712-wake-wannacry-attacks-un-cybersecurity-expert-discusses-internet-safety (accessed September 30, 2018)

[17] "In wake of 'WannaCry' attacks, UN cybersecurity expert discusses Internet safety" UN News, https://news.un.org/en/story/2017/05/557712-wake-wannacry-attacks-un-cybersecurity-expert-discusses-internet-safety Christina Lam

[18] "In wake of 'WannaCry' attacks, UN cybersecurity expert discusses Internet Safety", UN News.

[19] "Lessons Learned Review of the WannaCry Ransomware Cyber Attack" U.K. Department of Health and Social Care, https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf (accessed October 11, 2018).

[20] "Lessons Learned Review of the WannaCry Ransomware Cyber Attack" U.K. Department of Health and Social Care.

[21] "In wake of 'WannaCry' attacks, UN cybersecurity expert discusses Internet Safety", UN News.

[22] "Learning to Improve Resiliency Against Cyberattacks" The Hill, https://thehill.com/opinion/cybersecurity/406269-learning-to-improve-resiliency-against-cyberattacks (accessed October 7, 2018).

[23] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History" Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed October 7, 2018).

[24] "Learning to Improve Resiliency Against Cyberattacks," The Hill.

[25] "The White House Blames Russia for NotPetya, the most Costly Cyberattack in History" Wired, https://www.wired.com/story/white-house-russia-notpetya-attribution/ (accessed October 11, 2018).

[26] "The White House Blames Russia for NotPetya, the most Costly Cyberattack in History" Wired.

U.S. Democratic National Committee (DNC) which resulted in documents, campaign information, and 20,000 private emails being leaked to the public.[27] U.S. intelligence agencies have since accused the Russian government of being responsible for these attacks.[28] Russia has in return denied any responsibility for these cyber-attacks and has threatened sanctions against the U.S. due to these accusations.[29] U.K. Prime Minister, Theresa May, has also accused Russia of election meddling, but Russia continues to deny these accusations.[30] There has been no repercussion placed on the Russian Federation, or any other suspected Member State in response to this attack.

The risk penetrates further, right down to the individual user as private citizens have reported being victimized by a cyberattack. In the first six months of 2017 alone, almost 2 billion data records were lost or stolen, affected millions of individual citizen. [31]When social media sites like Facebook are hacked, millions of users' personal information could be accessed by the perpetrators.[32] The October 4, 2018 Facebook hack affected over 50 million users and took almost 11 days to stop. [33] Other major hacks have included the attack on the credit reporting firm Equifax and the dating site Ashley Madison, both of which resulted in the leak of millions of users' personal information.[34]

The Security Council is primarily tasked with preserving international peace and security, which includes cyber security.[35] In 2017, the United Nations Security Council passed Resolution 2341 unanimously in order to further "encourage all States to make concerted and coordinated efforts, including through international cooperation, to raise awareness and expand knowledge of challenges posed by terrorist attacks, so as to be better prepared for such attacks."[36] The purpose of this resolution is also to encourage Member States to share best practices for managing the threat of cyber-attacks which target critical infrastructure such as powerlines, airports, nuclear power plants, hospitals, etc.[37]

Even with Resolution 2341, Member States are still vulnerable to these vicious attacks. These cyberattacks have the capability to spread beyond boarders placing millions of people and businesses at risk. Between 2016 and 2017, data breaches increased 164 percent.[38] The lack of international response to these wide-spread attacks is likely contributing to their exponential increase. As cyberattacks continue to rise, it is imperative that the UN Security Council work to ensure Member States have protections in place to defend against these attacks.

---

[27] "A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election" Christina Lam, (accessed September 30, 2018)

[28] "A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election" Christina Lam, (accessed September 30, 2018)

[29] "A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election" Christina Lam, (accessed September 30, 2018)

[30] "Theresa May Accuses Vladamir Putin of Election Meddling" BBC, https://www.bbc.com/news/uk-politics-41973043 (accessed October 7, 2018).

[31] "The Number of Cyberattacks is surging- and it's Likely to Get Much Worse" CNBC, https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html (accessed October 11, 2018).

[32] "Facebook Just Had its Worst Hack Ever – and it Could Get Worse" CNN Business, https://www.cnn.com/2018/10/04/tech/facebook-hack-explainer/index.html (accessed October 9, 2018).

[33] "Facebook Just Had its Worst Hack Ever – and it Could Get Worse" CNN Business, (accessed October 9, 2018).

[34] "Facebook Just Had its Worst Hack Ever – and it Could Get Worse" CNN Business, (accessed October 9, 2018).

[35] "The Security Council" United Nations Security Council http://www.un.org/en/sc/ (accessed September 15, 2018)

[36] "Security Council Calls on Member States to Address Threats against Critical Infrastructure, Unanimously Adopting Resolution 2341" United Nations, (accessed September 15, 2018)

[37] "Security Council Calls on Member States to Address Threats against Critical Infrastructure, Unanimously Adopting Resolution 2341" United Nations, (accessed September 15, 2018)

[38] "The Number of Cyberattacks is surging- and it's Likely to Get Much Worse" CNBC.