COMMITTEE: United Nations Cybersecurity Committee

TOPIC: combatting state-sponsored hacking

MAIN SUBMITTER: China, Côte d'Ivoire, Peru, Thailand

CO-SUBMITTER: Turkey, Kuwait, Israel, USA, Dominican Republic, Italy, South Korea, Germany, Iran, DPR Korea, Equatorial Guinea, Canada, Pakistan, South Africa, Mexico, Saudi Arabia, France, India, Portugal, Austria, Morocco, United Kingdom

THE GENERAL ASSEMBLY,

*Recognizing* states' utilization of technologies to hack into other groups, countries, or Member States for illicit reasons,

*Understanding* that the younger generations play large roles in current cybercrimes and hacking,

*Acknowledging* the large amount of cyberattacks and hacking that is originating in less economically developed nations as well as more economically developed nations,

*Understanding* that cyber attacks are inevitable,

*Aware* that many people worldwide are being targeted by cybercrimes, and that a large percentage of them are being inhibited from continuing their lives as they had been,

*Bearing in mind* that many small, medium, and large businesses are being harmed by cyberattacks and hacking,

*Noting* that many antiviruses are inefficient and may leave technologies more vulnerable to cyberattacks,

1. Stresses the importance of developing consequences to deter states from participating in or sponsoring any hacking activities or being accessories to hacking crimes as well as funding such operations:
    a. Punishments for such crimes will vary depending on the severity of the crime and which of the seven levels of hackers is being helped by the state, with the punishments generally following:

i. Funding of script kiddies and hacking groups is typically inconsequential for other countries; hence, it does not require punishment, as these attacks fail or have little to no effect,

ii. Hacktivists such as the groups Anonymous and Turkish Hacktivists are able to cause political and economic turmoil within a country and the sponsoring of these people calls for a degree of intervention on the part of the government:

1. State officials who take part in the sponsoring must be apprehended,
2. Requires warnings to not participate in the activity again or require punishments such as limited jail time or fines,

iii. Black Hat Professionals (i.e. those with malicious intent and highly capable in their use of IT) necessitate harsher punishments given the gravity of their offences and the impact of these,

iv. Organized Criminal Gangs are led by a professional while the rest of the group is less advanced in hacking. However, the gangs are extremely dangerous due to the knowledge of the professional leader. The funding of such a gang calls for immediate action against the Member State's government in order to prevent further harm and for the implementation of very significant jail time and fines against the officials who took part in the action,

v. Nation States, the next level of hacking, with groups such as Stuxnet, must be monitored as their hackers are paid by said Nation States consistently and are highly trained. If ever the trained hackers are used against other countries during times of peace, then sanctions must be created to stop the actions of the Nation State, including cutting funding from the CFAD,

vi. The Automated Tool can severely damage a country and its information. These attacks have severe consequences on the victim and affect the world, hence the necessity of harsh punishments such as lengthy jail times and extensive fines, and in those cases where it is used against another country during times of peace, heavy sanctions are required,

vii. The punishment also depends upon the severity of the perpetrated act, as higher levels of hackers may take part in lesser crimes, calling for less severe actions against them,

2. Encourages the development of a treaty for Member States to sign which details international rules that would prohibit state sponsored hacking:

a. Member States will be required to address any accounts of state sponsored hacking within their own regions in order to prevent any further issues before they form,

b. Member States must agree to sanctions being placed depending on the severity of the effects of the sponsored hacking on other nations,

c. Member States which fail to abide by the terms stated in the treaty will be faced with sanctions placed upon them by other Member States,

d. As defined by the U.S. Federal Bureau of Investigation, cyberterrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by sub-national groups or clandestine agents."

3. Advises businesses and corporations as well as the general public to increase education and awareness of employees in regards to the increasing likelihood of a cyberattack:

a. Ensuring employees are aware of possible hacking allows for better understanding within the workplace and leads to smoother processes if hacking occurs,

b. Employees must make it known if they ever encounter a possible hacking issue or any likelihood of one,

c. Trying to make the general populace more technologically literate by implementing programs in educational institutions,

d. Encouraging cyber exercises, noticing the fact that they already proved their efficiency in other countries,

e. Employing buyers of a given product to read the terms of service in regards to their personal privacy and collected information,

f. Imposing regulations over children’s downloadable content that may violate their personal devices or information on that system,

g. Affiliate with websites that are either educational (.org) or are secured,

4. Urges private security practices related to updating software to be taken:
    a. Old software is easily accessible for hackers and makes information more available to them,
    c. Businesses and those who have to worry about hacking must retain the most up to date software as it is safer, more reliable, and they tend to have better security,
5. Encourages the use of firewalls, antiviruses, and antispyware in order to increase security of technology to prevent hackers from easily accessing data:
    a. Member States and businesses must ensure that each application within the government and businesses is updated as older technology is more easily accessible to hackers,
    b. Those who are hacked must act immediately when the firewall is breached to prevent further damage and to secure any important data,
6. Calls Upon expert help during those times when a Member State is hacked, or the Member State should hire an expert on hacking prevention to remain within the government to address hacking issues when they occur:
    a. Hackers will be less likely to attack when they know that an expert is at hand, decreasing the likelihood of an attack,
    b. When attacks occur, the expert at hand will be enabled to address it immediately and even possibly have the opportunity to find the hacker responsible,
7. Requests that those with important information, and even those without, consistently fix any technical issues immediately when they occur in their devices:
    a. Viruses and other issues within devices make the device more easily accessible to hackers,
    b. By resolving issues within the device when they occur, the possibility of hacking does not increase and may decrease,
8. Endorses the safeguarding of secrets within government and business bodies in order to protect any important information which would be detrimental for hackers to discover and possibly release to a broader audience:
    a. It is required that those with sensitive information consistently change passwords when a breach of access is made aware with the new password being significantly different from the previous

b. Encrypt customer data:

i. It is catastrophic for both the business and customer if customer data is compromised, hence the necessity of ensuring hackers cannot see the data even if a business is hacked,

ii. Customers' financial data should always be outsourced,

iii. Passwords should never be encrypted, but hashed,

9. Requests United Nations funds to be allocated to developing nations for the purpose of developing cyberdefense infrastructures:

a. Funding will be gathered from all member nations,
b. A committee called the Committee for Allocation of Funds for Cyber-Attack Defense (CAFCAD) will be created to determine on a case-by-case basis how much funding is necessary for each country to expand its defense to the necessary level as well as other cyber security related issues.
    i. The CAFCAD will reassess needed funds for each country annually, and funding will be given continuously as defense systems are a constant problem,
    ii. If determined necessary, the CAFCAD will have the ability to allocate expert personnel to aid the development of cyber defence infrastructure,
    iii. The committee handles overseeing cooperation between nations on the research and development of cyber defense technologies,

10. Calls upon Member nations to develop internal defense systems (with the aid of the United Nations where necessary):

c. Nations must realize that they are at risk and assess the extent to which they must fortify their defenses,
d. In an effort to streamline the process and improve the efficiency of cyber defense systems, nations should create internal agencies dedicated to the defense of cyber assets,
e. Said agency would be responsible for protecting high priority cyber targets within the nation, and through the cooperation of the nation, improve the quality of their national defense,
f. Nations should work with cyber companies domestically and internationally to develop software that will deter hackers, as well as a system of determined notification to countries in a position of peril,
g. Countries are encouraged to make the necessary internal changes to identify domestic attacks on themselves or other nations,
h. Nations are encouraged to cooperate with each other on the research and development of cybersecurity technology,