Issue Brief
(GA6)

Cybercrime

With the speedy innovations and development in the field of technology in the 21st century, crime is no longer bound to physical interaction but has evolved to adapt to the increase on dependability on technology in a digital age. Cybercrime is a transnational form of crime that many criminals abuse due to its speed, convenience and most importantly its anonymity. Previously, cybercrime was committed by small groups and individuals, however today we are witnessing highly complex cybercriminal networks working together and committing crimes on an unprecedented scale. With more people on the internet and exposed to the cyberspace, the issue of cybercrime becomes more pertinent and combating it critical.

Cybercrime can be divided into two forms, advanced cybercrime and cyber-enabled crime. Advanced cybercrime is the effective attack by hackers, be it individuals or organizations, on computer software and hardware, where they breach and infiltrate computers without a right and cause damage directly or indirectly in addition to information theft and harvesting. On the other hand, Cyber-enabled crime is the criminal society's adaptation to the digital age to commit their traditional crimes through the cyber realm; these would include crimes against children, financial crimes and even terrorism.

The main United Nations body that targets the growing concern of cybercrime is the United Nations Office on Drugs and Crime (UNODC), where it promotes sustainable measures and policies to limit cybercrime in both national and international levels. In addition to the issue of combating cybercrime is the issue of jurisdiction. Because cybercrime by nature is transnational and victims of cybercrime can be in other states it places an obstacle for law enforcement. The United Nations plays a major role in state-to-state dialog and for international laws and criminal justice in this transnational issue. Among the methods the UN engages in to combat the growing issue of cybercrime is they active provision of education for police and prosecutors on how to investigate cyber based crime, money laundering, and terrorist financing and aiding governments realize what that threat is, what it looks like, and how they can act politically, through legislation, and through reaction, to counter that threat. Due to the transnational nature of cybercrime and its increasing concern the United Nations is a key actor with the most potential and power in the fight against cybercrime.

Ahmad Al-Naimi
President of the General Assembly