Use of Internet Technology to Facilitate Communication in Planning International Crimes

Anjali Jain
U2103281- M100 Law LLB
ORCID iD- 0009-0005-1916-4157
URSS
UNDERGRADUATE RESEARCH SUPPORT SCHEME
THE UNIVERSITY OF WARWICK
Supervised by Prof. Solange Mouthaan

Planning International Crimes

The planning of international crimes represents a highly clandestine and intricate aspect of criminal strategies and activities that and conducted by organised crime groups across borders. These organisations efficiently exploit the vast capabilities of the growing internet technology to strategies and orchestrate their operations with remarkable precision often eluding the grasp of law enforcement agencies. This phase is the foundation of criminal activities ranging from terrorism and drug trafficking to money laundering, human trafficking and cybercrime.

Use of Internet Technology by Crime Organisations

Mediums Used

Blogs and Websites- The International Criminal Police Organisation (INTERPOL) highlighted the extensive use of websites for communication and suggested that more than 100 websites were monitored on a daily basis for any kind of terrorist content.

Steganography- Known for significantly being used by ISIS and Al-Qaeda, is a practice of hiding messages or information within seemingly innocuous files, such as images or documents and has been known to be a favoured method of hiding sensitive data from security and regulatory bodies.

Satellite Phones- Reports to the United Nations, Satellite phones have notably been used by pirates operating in the Indian Ocean, significantly for coordinating illicit activities and evading traditional communication networks.

Use of Dead Drops- It is often used for anonymity and reducing the risk of digital detection, especially in the context of espionage, intelligence operations, or illicit activities.

Burner Phones- Pew Research's report shows that 68% of the American population has utilised burner phones as a means to safeguard their privacy.

Human Couriers- Human Couriers have been employed throughout history, often during wars and crimes when it is important to have secure and covert communication. This is a crucial method for espionage, intelligence operations and resistance movements.

Infiltration and Insider Threats- Reports by Accenture have shown the prevalence of these attacks and revealed how over two-thirds of organisations across the globe have encountered incidents involving insider threats.

Un-regulated Apps

Gaming Platforms- Newzoo's Report demonstrated the widespread adoption of online gaming and that there were over 2.7 billion gamers in 2020 worldwide.

Dating Apps – According to Statista, Tinder alone has over 30 million users, this underscores the extensive reach and influence that dating apps have within the digital landscape.

Educational Apps- The use of educational apps for illicit activities underscores the adaptability and creative tactics employed by these organisations to maintain secrecy and evade traditional surveillance methods.

Similarly, anonymous chat apps like Kik and Wickr are favoured for covert conversations, yet statistics on their criminal use are not readily available. Social media aggregator apps, which enable efficient monitoring and communication across various platforms. In the context of the COVID-19 pandemic, video conferencing apps like Zoom experienced a significant increase in users, surpassing 300 million daily meeting participants in 2020 where the platform was adopted for both legitimate and illicit purposes.

Mediums used for facilitating crimes

Communication and Coordination- Reports by Europol, the use of these services has been increasing with a particular focus on privacy-focused apps like Signal and Telegram. In a survey by Atlas VPN in 2021, it was found that 61% of respondents worldwide used VPN, illustrating the widespread adoption of these services for various purposes including illicit ones.

Cybercrime- Cybersecurity Ventures in 2021 predicted cybercrime damages to reach $6 Trillion on an annual basis after the FBI's Internet Crime Complaint Centre (IC3) reported cybercrimes that were a cause of over $4.2 Billion in financial losses for the victims of United States alone.

Money Laundering- Cryptocurrencies, including Bitcoin, were estimated to have been used in 1% of all global money laundering cases as per reports of the Financial Action Task Force (FATF) and in 95% of all terrorist transactions in 2020 as per reports by the International Centre for Counter-terrorism (ICCT).

The United Nations Office on Drugs and Crime (UNODC) came down to an estimated rough figure that between $800 Billion- $2 Trillion in criminal proceeds are laundered annually, most of it facilitated through online financial systems.

Terrorist Financing- ISIS alone generated over $2 billion from looting bank assets, kidnappings, and extortion from 2014 to 2016 (U.S. Department of State).

Fraud and Scams- As per the Data Breach Investigations Report by Verizon, Phishing attacks account for up to 80% of all reported cybersecurity incidents. The Federal Trade Commission (FTC) received over 2.2 million reports of fraud and scams in 2020 in the United States which would come up to $3.3 billion in losses.

Illegal Online Marketplaces- Research by RAND Corporation found that the dark web's illegal marketplace revenues surpassed $300 million annually in the year 2015 and later in 2021, found in a report by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) that over 700 dark web marketplaces, where various illegal goods and services were being traded.

Digital Extortion- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) noted a 300% increase in ransomware attacks that were reported in 2020 and 2021 these attacks were projected to reach $ 20 Billion by cybersecurity ventures.

Human Trafficking- Human Trafficking is one of the most profitable criminal enterprises generating about $150 Billion annually [estimates of the International Labour Organisation (ILO)].

Cyber Espionage- The FBI's Internet Crime Complaint Centre (IC3) saw a significant hike in cyber-espionage cases with over 108,000 reported incidents in 2020.

Disinformation and election interference – In 2020, the European Union's East StratCom Task Force identified and catalogued more than 7,000 disinformation cases in 2020, including attempts to interfere with elections and manipulate public opinion. The Internet Research Agency, a Russian organisation was also seen reaching out to Americans through its social media disinformation campaigns during the 2016 presidential elections (U.S. Senate Intelligence Committee).

War Crimes Documentation- The Syrian Archive which is a non-profit organisation documented over 3,000 incidents of war crimes in Syria through open-source investigations. In 2020, a Congolese Warlord was convicted by the International Criminal Court (ICC) based on a shred of extensive video evidence, demonstrating the increasing use of digital technology in war crimes prosecutions.

Online Piracy and intellectual property theft – In 2020, the Motion Picture Association reported $29.2 billion of revenue loss to online piracy by the global film and television industry. The Global Innovation Policy Centre (GIPC) has also estimated a value of $200 billion in intellectual property theft costs in the U.S. Economy.

Influencing

Social Network and Relationships- Studies by the National Institute of Justice have shown that 88% of recruits are introduced by their close acquaintances to the criminal lifestyle.

Peer Pressure- The National Gang Centre shows that peer pressure is cited in over 30% of gang-related cases by glamorising the criminal lifestyle by making it appear attractive and impressionable.

Economic Incentives- reports by the United Nations Office on Drugs and Crime suggest that around 60% of recruits have been motivated to join by its economic incentives.

Vulnerable Youth- Approximately 63% of gang recruits are adolescents as per the National Gang Centre

Social Media- Statistics provided by the Centre on National Security at Fordham Law suggest that over 70% of recruitment in extremist groups occurs through online channels.

Ideological Narratives and Manipulation- As per the International Centre for Counter-terrorism manipulation was a significant motivating factor depending on the context for 23% to 60% of recruits.

Threats- Up to 49% of recruits are pressured or threatened to be a part of their community as shown by reports from The International Centre for Counter-Terrorism