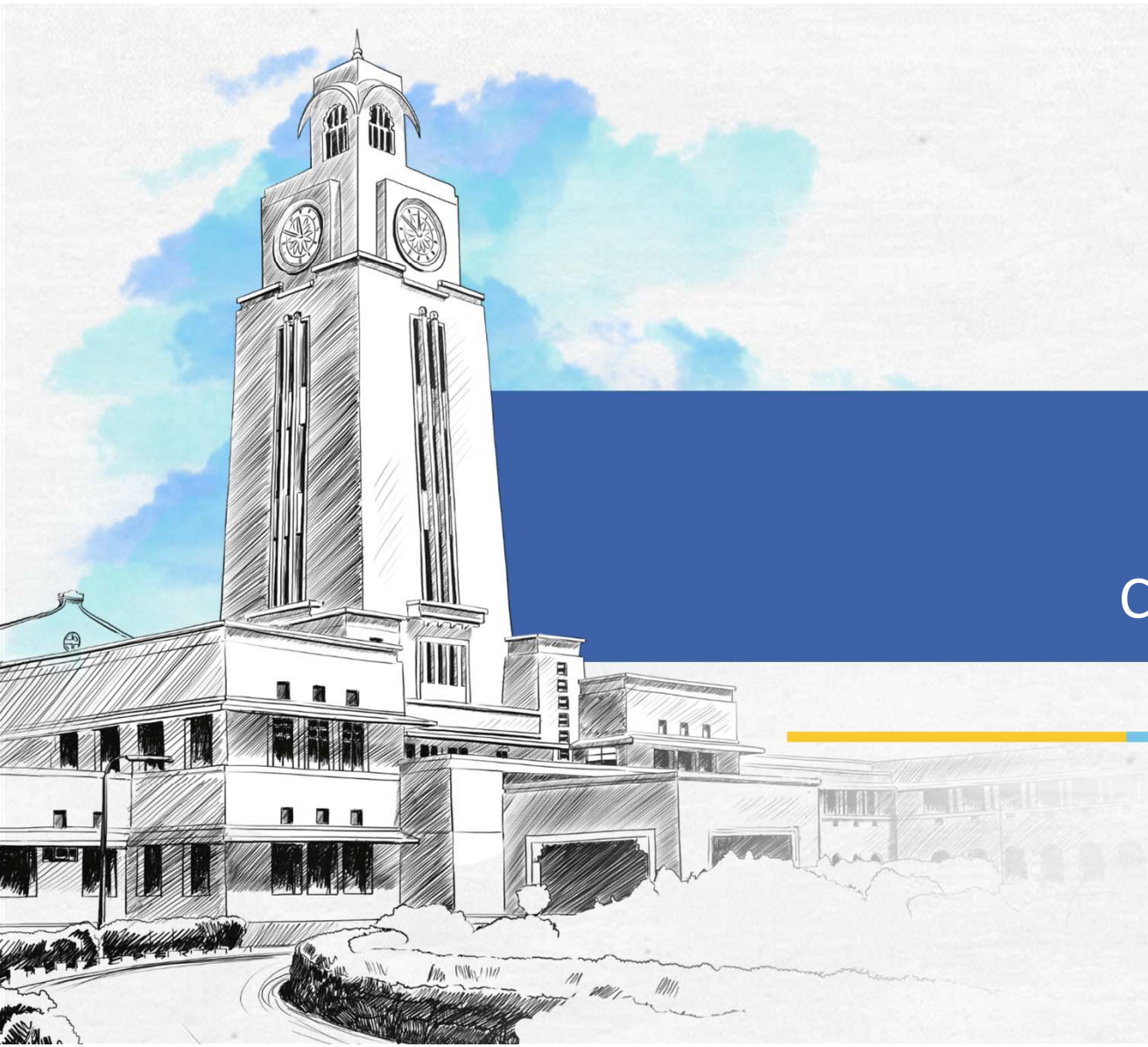


BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Cyber Crimes and Offenses

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Common Cyber Attacks

innovate achieve lead

Agenda

- Cyber Crimes and Offenses:
  - Introduction to Cyber Crimes
  - Motives
  - Classification of crimes and criminals
  - Types, frequency and amount of Cyber Crime
  - Organized Cyber Crime
  - Cyber terrorism
  - Cyber war
  - Cyber Crime Modus-Operandi and Social Engineering
  - Cybercrimes against individuals, organizations, and nations
  - Cyber Crime Techniques
  - Cyber Crime Monitoring and Prevention
  - Domestic and International Response

Organized Cybercrime

Organized Cybercrime

innovate achieve lead

Introduction

- Many crimes and cybercrimes have some level of organization
- These crimes are:
  - "planned, rational acts that reflect the effort of groups of individuals"
- Two basic questions to be answered:
  - What role does cyberspace play in helping criminals organize themselves?
  - How does cyberspace and its technologies transform organized criminal behavior to create new forms of crime?

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Cyberspace and the organization of criminal groups

- The activities of terrorists and organized criminal groups can overlap, but, their objectives are different
  - Terrorists primarily pursue political or social objectives
  - Organized criminal groups primarily pursue "financial or other material benefits"
- Most organized criminal groups use the Internet technologies to organize themselves to some extent
- These groups tend to exist in three levels
  - ephemeral (short term)
  - sustainable (long term with proper organization)
  - hybrids (somewhere in-between)

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Cyberspace and the organization of criminal groups

- Ephemeral
  - They use Internet technologies just to communicate with one another and conduct their "business"
  - The use of Internet is to the extent of connecting offenders for committing the crime offline
  - Once the work is done, they dissipate to form new alliances
- Sustainable
  - Organized criminal groups may use networked technologies to create more "sustained" organizational forms
  - These organizational forms are meant to last in time
  - They offer protection to the criminals operating under its wing from other criminals in the field and also law enforcement agencies
- Hybrids
  - In hybrid forms, criminal goals are widely circulated 'virtually' by a small core group
  - These goals are implemented by individual groups or local cells such as hacker groups

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Cyberspace and the organization of cybercrime

- All organized criminal groups use some type of networked technology
  - to organize themselves and their crimes
- Some groups use these technologies to commit cybercrimes
- The actual nature of how cybercrimes are organized depends on three aspects:
  - the level of digital and networked technology involved,
  - the modus operandi, and
  - the intended victim groups

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Cyberspace and the organization of cybercrime

- The level of digital and networked technology involved
  - Traditional organized criminal groups tend not to be involved in committing cyber-dependent crimes
    - Because these crimes disappear when the Internet is removed
  - These groups, however, increasingly use networked technologies to communicate with each other to organize crimes or seek intended victims
    - For example, to sell drugs over the Internet or darknet
  - These forms of cybercrime are either
    - cyber-assisted
    - cyber-enabled
    - cyber-dependent

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Cyberspace and the organization of cybercrime

- The level of digital and networked technology involved
  - cyber-assisted
    - The technology is used for communicating among the members
    - Without the Internet the offense would still take place but by other means of communication
  - cyber-enabled
    - Here, the long-standing (usually localized) forms of offenses, such as illicit gambling, frauds and extortion, are given a global reach by digital and networked technologies
    - If the Internet is removed, then the offending would revert from the global to the local form
  - cyber-dependent
    - Crimes such as hacking, DDoS, ransomware, attacks, and spamming
    - These disappear when the Internet is removed from the equation

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Cyberspace and the organization of cybercrime

- Modus Operandi
  - Organization of cybercrime also varies according to the modus operandi of the offense involved
    - Modus operandi is linked with the motivations and profile of the criminal actors
  - Three levels of organizations are possible depending on how the computer is used
    - cybercrimes against the machine
      - E.g., computer misuse offences by hackers
    - cybercrimes using the machine
      - E.g., scams, frauds, and extortion
    - cybercrimes in the machine
      - E.g., child sexual abuse material, hate speech, terrorist material

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Cyberspace and the organization of cybercrime

- Target Victim Groups
  - Some criminal groups target individual users
    - E.g., spamming deceptive emails to scam or defraud them
  - Other groups target businesses or governmental organizations, to commit larger scale frauds
    - E.g., obtain trade secrets or to disrupt their business flows (ransomware)
  - Finally, other groups (State actors), target the infrastructures of other States
    - E.g., power grids, nuclear plants, etc.,.
- Thus, the organization of cybercrime depends upon
  - the level of technologies used,
  - the particular criminal acts being committed, and
  - the intended victim groups.

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Conceptualizing organized crime

- The United Nations Office on Drugs and Crime (UNODC)
  - Established in 1997 as the **Office of Drug Prevention and Crime Prevention** by combining the **United Nations International Drug Control Program** (UNDCP) and the **Crime Prevention and Criminal Justice Division** in the United Nations Office at Vienna
  - It was renamed the United Nations Office on Drugs and Crime in 2002
  - The agency's focus is drug trafficking, abuse of illicit drugs, crime prevention and criminal justice, international terrorism, and political corruption It
  - In 2016–2017 it had an estimated biannual budget of US$700 million.
- The United Nations Convention against Transnational Organized Crime
  - This convention is UNDOC's main international instrument in the fight against transnational organized crime
    - https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html
  - Provides a list of offenses conducted by criminal groups
    - https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Conceptualizing organized crime

- Definition of Organized Criminal Group
  - According to The United Nations Convention against Transnational Organized Crime, "Organized criminal group" is defined as
    - *"a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit."*
  - Here, a structured group
    - does not need a formal hierarchy or continuity of its membership
  - This makes the definition broad, including loosely affiliated groups without any formally defined roles for its members or a developed structure

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Conceptualizing organized crime

- Definition of Organized Crime
  - There is no universally agreed upon definition of organized crime.
  - It can be understood as
    - *"a continuing criminal enterprise that rationally works to profit from illicit activities that are often in great public demand. Its continuing existence is maintained through corruption of public officials and the use of intimidation, threats or force to protect its operations"*
- Definition of Cyber Organized Crime
  - By extension, cyber organized crime is a term used to describe organized crime activities in cyberspace
  - Like organized crime, there is no consensus on the definition of cybercrime or cyber organized crime

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Conceptualizing organized crime

- Three features are prominent with organized crime
  - Control of Territory
  - Corruption
  - Use of Violence or Threat

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Conceptualizing organized crime

- Control of Territory
  - Some of the traditional features of organized crime may not translate well to cyberspace
  - For example: "control of territory"
    - An organized criminal group attempts to regulate and control the "production and distribution of a given commodity or service" unlawfully
  - This regulation is present in dark markets (E.g., the defunct DarkMarket and CardersMarket on the Internet), where
    - administrators and moderators monitor site and content and ensure rules of the platforms are enforced
    - If rules are not obeyed, those engaging in non-compliance are excluded from the site
  - While "the production and distribution of a given commodity or service" could be controlled within these sites, this control does not extend to other online forums (thus limiting the power and authority of the networks)

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Conceptualizing organized crime

- In the case of dark markets, the structure, organization, regulation, and control over illicit goods and services are connected to the online sites and not the people who run and/or moderate them
- When these dark market sites are taken offline (by law enforcement), the network associated with this site often ceases to exist
- However, there are exceptions to this, where members (those not caught by the law enforcement) have created another site that mirrors the one taken offline
- A case in point is the darknet site Silk Road 2.0 (now defunct)
  - Silk Road 2.0 mimicked Silk Road
  - Silk Road 2.0 was created to maintain continuity of activities previously performed on Silk Road
  - Even the name of the administrator, Dread Pirate Roberts, remained the same as the one used by the administrator of Silk Road (at least before the administrator was arrested)
- Silk Road
  - **Silk Road** was an online black market and the first modern **darknet** market, best known as a platform for selling illegal drugs
  - As part of the **dark web**, it was operated as a **Tor** hidden service, such that online users were able to browse it anonymously and securely without potential traffic monitoring

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Conceptualizing organized crime

- Silk Road
  - https://www.youtube.com/watch?v=eLOSVAJH2ks
- THE DARK WEB | SILK ROAD – Explained
  - https://www.youtube.com/watch?v=lFZLjJooBys
- What is the Dark Web?
  - https://www.youtube.com/watch?v=fUjSVrh9UN4

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Conceptualizing organized crime and defining the actors involved

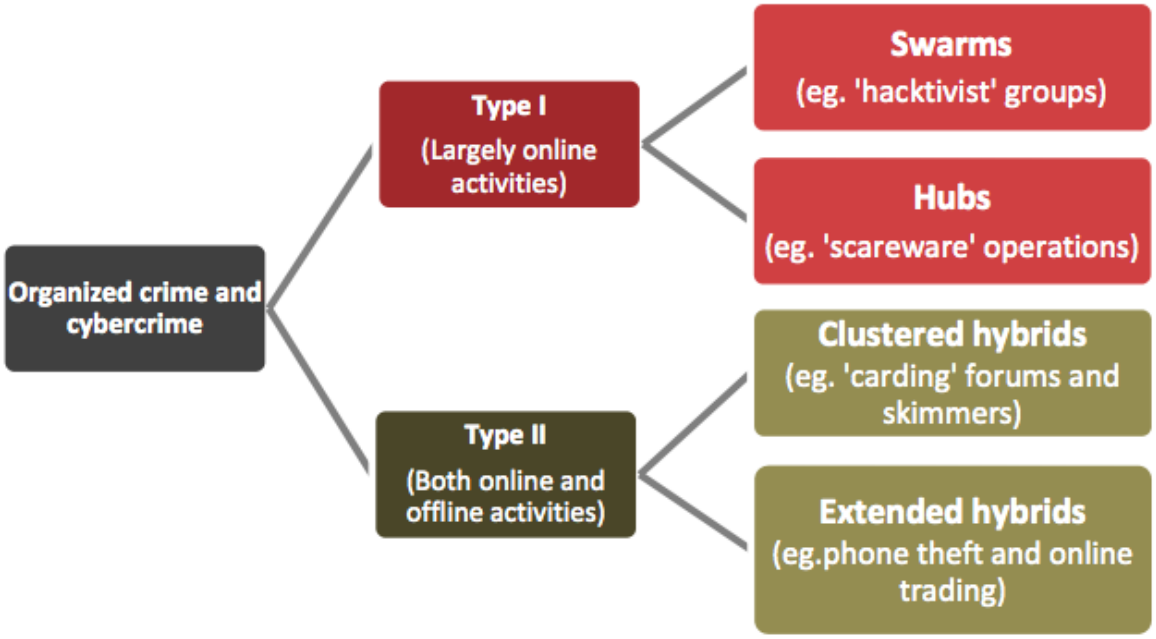
- Corruption
  - Political corruption influences decisions to participate in organized crime activities
  - In one country, online fraud, among other financial crimes, were found to be integral to the functioning of the State
- Use of violence or threat of the use of violence
  - There is no evidence of the use of threat or violence in furtherance of cyber organized crime activities
  - However, cyber organized criminals conduct or threaten cyberattacks or other forms of cybercrime as a means to coerce individuals into complying with demands
  - For example: Cyber organized criminals use
    - cryptoransomware (i.e., malware that infects a user's digital device, encrypts the user's documents, and threatens to delete files and data if the victim does not pay the ransom)
    - doxware (i.e., a form cryptoransomware that perpetrators use against victims that releases the user's data…if ransom is not paid to decrypt the files and data)

Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Organization Types



Source: BAE Detica/LMU

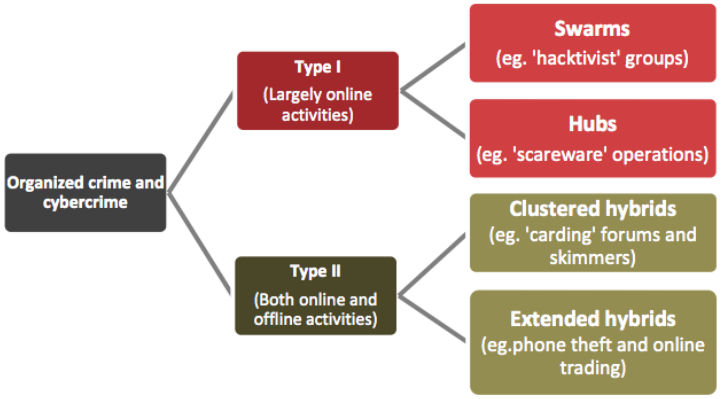
Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime

innovate achieve lead

Organizational Types

- Type-I
  - Type I groups operate almost completely online
  - Groups falling into this category are generally composed of autonomous individuals
  - These individuals do not necessarily have a structure in the same way that a traditional organized crime group might
  - Type I organizations can be broken down further
    - Swarms and
    - Hubs



Source: BAE Detica/LMU

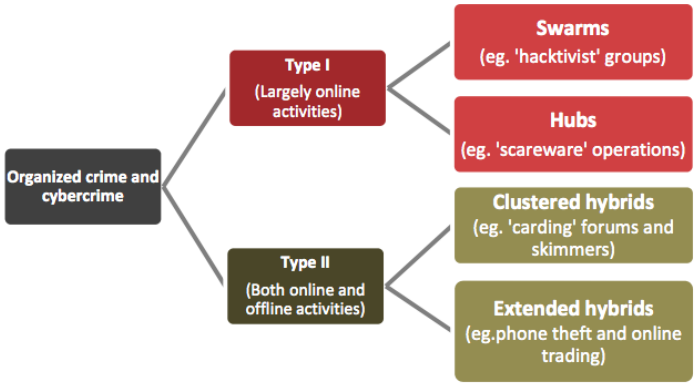
Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Organized Cybercrime

innovate achieve lead

Organizational Types

- Type-I: Swarms
  - Generally considered as the least organized of the group types
  - They operate as "leaderless resistance"
    - Group members may be operating on the same principles and be motivated by the same objectives
      - However, there is not a single individual or entity that controls any aspect of the organizations
    - In a sense, these groups are self-organizing
  - Swarms are short-term associations formed for a specific purpose and dissolved after their objectives are achieved
  - Swarms are one of the most difficult types of groups to combat, because
    - individual members may not know one another, and
    - there is no organization to disrupt
  - The best-known group that falls into the swarm typology is the hacker collective *Anonymous*



Source: BAE Detica/LMU

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Organized Cybercrime

innovate achieve lead

Organizational Types

- Type-I: Swarms
  - Swarms do not meet the strict definition of an organized criminal group
  - However, the group does conduct illegal, organized campaigns against different organizations, including governments
  - Because of its nature as a swarm, law enforcement has had a difficult time disrupting the collective
  - The group sometimes engages in activities that indirectly support law enforcement
    - many question whether the group should be targeted by law enforcement at all
  - Anonymous and many other collectives fit the swarm model

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Organized Cybercrime

innovate achieve lead

Organizational Types

- Type-I: Hubs
  - Hubs are more-structured groups than swarms that mostly operate online
  - Unlike swarms, hubs coalesce around a core group of individuals who may be considered leaders
  - The hubs often have a more clear command structure than do swarms
  - Organizations that are arranged as hubs take part in a significant amount of criminal activity
  - Examples of hubs include:
    - Silk Road, an online bazaar where illegal wares ranging from drugs to assassins can be found
    - Carders' markets, that is, markets where stolen credit cards are sold, and
    - Purveyors (spreaders) of scareware
      - malware that tricks people into buying useless or harmful programs by scaring potential buyers
  - These organizations develop, distribute, and collect money from programs (malware) that are developed
  - A small group of developers may enlist others to help spread the malware, or they may sell it on a marketplace and allow others to distribute it for their own profit

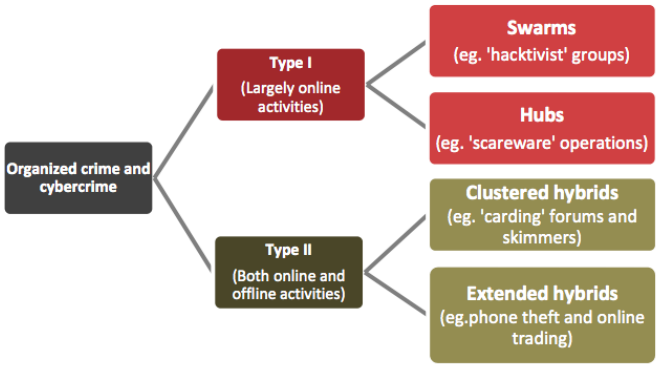
Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Organized Cybercrime

innovate achieve lead

Organizational Types

- Type-II
  - Type II groups combine online and off-line criminal activity
    - This makes them the most complicated form of organized criminal group
  - Type II organizations are also called "hybrids"
  - They can be subdivided into two types:
    - Clustered hybrids
    - Extended hybrids.



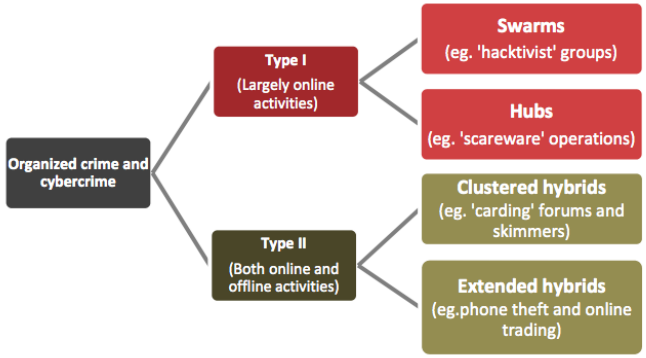
Source: BAE Detica/LMU

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Organized Cybercrime

innovate achieve lead

Organizational Types



Source: BAE Detica/LMU

- Type-II – Clustered Hybrids
  - Clustered hybrids resemble hubs in their structure
  - The main difference is that the clustered hybrids can operate across multiple environments, whereas a hub is only operational online
    - Because of this ability to operate across the online and real worlds, clustered hybrid organizations can be quite dangerous
  - A large number of groups follow this organizational model, and the groups engage in a variety of illicit activity, both online and off-line
  - For example:
    - Participating in illegal markets for credit card data or other information that can be sold
    - The cards may be stolen online or physically, and the information sold in online carders' markets

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Organized Cybercrime

innovate achieve lead

Organizational Types

- Type-II – Clustered Hybrids
  - Many of the hackers participating from the Russian side of the Russian/Georgian conflict were likely run by the mafia:
    - Russian organized crime
  - Terrorist organizations could develop the capacity to engage in this kind of criminal activity, both for fund-raising and operational purposes
    - For instance, Hamas, during the 2008 war with Israel, defaced a significant number of Israeli websites
  - Given Hamas's ability to operate in both the physical and online environments, it could be classified as a clustered hybrid organization
    - Although clearly it is not yet well developed in the online world

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Organized Cybercrime

innovate achieve lead

Organizational Types

- Type-II – Extended Hybrids
  - Extended hybrids (like clustered hybrids) operate seamlessly in both the online and physical environments
  - The key difference is that they are more diffuse (spread over a large number of people; not concentrated)
    - In this respect, they resemble a swarm more than a hub
  - However, they have the operational element that allows them to work in both the online and physical words
    - This makes them a Type II, rather than a Type I, organization

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Organized Cybercrime

innovate achieve lead

Organizational Types

- Type-II – Extended Hybrids
  - This operational group perhaps engages more in child pornography
  - Generation of such material occurs in the physical environment and then is exchanged in a variety of online forums
  - Unlike clustered hybrids, the extended hybrid model also allows for subunits to form and operate nearly independently of the original organization
    - For example, a small group of producers can control the online generation of content, but beyond this the diffusion of the illicit material is outside their control
  - Extended hybrid organizations remain much more autonomous than clustered hybrids

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!