



FIGHTING AGAINST CYBERCRIME ORGANISATIONS

**Palesteanian & Turkish Joint Conference On «Digital Evidences within
the Context of the Requirements of Investigation and Human Rights»
11-13 April 2019 in Ramallah**

DR. MURAT VOLKAN DÜLGER

***Assoc. Prof. Of Criminal Law and It Law
Istanbul Aydın University School of Law***

CYBERCRIME

- Definition: “Unlawful acts wherein the computer is either a tool or target or both”
- For an act to be classified as a cybercrime:
 - The conduct must be facilitated by *information and communications technology*;
 - The conduct must be motivated by *intent* to commit *harm* against a *person or organization*;
 - The perpetrated or intended harm must encompass conduct amounting to *interference or damage* to either *tangible or intangible property* owned by a person or organization; and
 - The conduct concerned must be *criminalised* within either the *jurisdiction of the victim* or the *jurisdiction of the accused*

CRIMINAL ORGANISATION

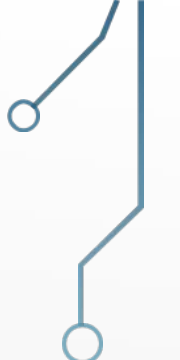
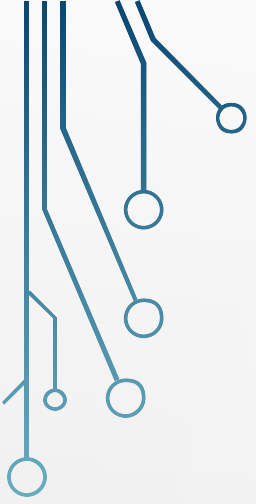
- Definition: “Any group that uses planning and group interaction in the furtherance of a criminal enterprise”
- United Nations Convention against Transnational Organised Crime:
 - *«a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing 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»*

CRIMINAL ORGANISATIONS IN THE CYBER SPACE

- There are mainly two types of criminal groups:
 - (1) the groups which consist of skilled technicians who use their knowledge and computer skills for engaging in cybercrime (the crimes which the group is engaged are cybercrimes)
 - (2) the conventional crime groups who have started to make use of digital technology in furtherance of criminal objectives (organised groups which utilise computer resources to conduct traditional crimes)

CRIMINAL ORGANISATIONS IN THE CYBER SPACE

- According to a research up to 80% of cybercrime could be the result of some form of organised activity. (McGuire 2012)



STRUCTURE OF CYBERCRIME ORGANISATIONS

(RODERIC BROADHURST/PETER GRABOSKY/MAMOUN ALAZAB/STEVE CHON, 2014)

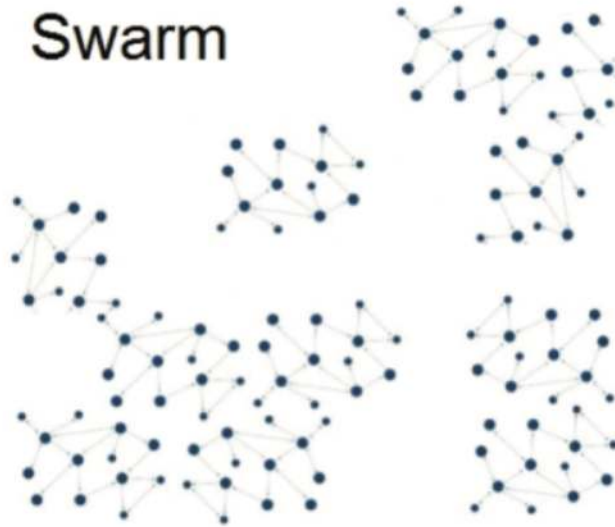


DOÇ. DR. MURAT VOLKAN DÜLGER



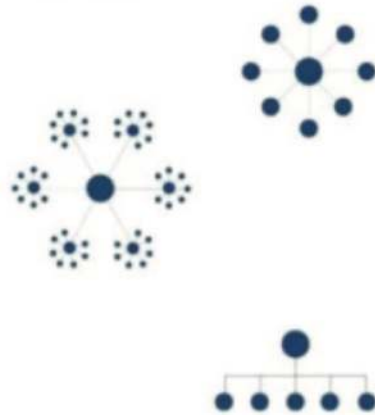
- There are six types of group structure (McGuire 2012)
- **Type I Groups:** These groups substantially operate online.
 - **Swarms:** They are defined as “disorganised organisation with common purpose without leadership.” Their chain of command is typically at the minimum level. Swarms mostly engage in ideologically driven online activities like hate crimes.
 - **Hubs:** Comparing to swarms, they are more organised with a clear command structure. Hubs consist of a focal point of core criminals and peripheral collaborators around it. They carry out wide range of online criminal activities, *inter alia*, piracy, phishing attacks, botnets and online sexual offending

Swarm



Large collective, disorganized, typically consisting of ephemeral clusters of individuals. For example, Anonymous has properties of a swarm.

Hub



Central command structure that can be hierarchical. Strong ties or continued interaction between individuals. For example, LulzSec has properties of a hub.

- **Type II Groups:** These groups are engaged in both online and offline offending.
 - **Clustered Hybrid:** In these groups, offending is enunciated around a small group of individuals and focused around specific activities or methods. They are structure-wise relatively similar to the structure of hubs; however, they move smoothly between online and offline offending. Commonly clustered hybrids engage in skimming credit cards and using the data for monetary purposes thereafter.
 - **Extended Hybrid:** They are less centralised comparing to clustered hybrids, but they operate similarly. They have an adequate level of coordination to realise their operations. Extended hybrids conduct various criminal activities by many associates and subgroups.

- **Type III Groups:** These groups predominantly operate online; however, they use online technology to facilitate and further their offline activities.
 - **Hierarchies:** These are traditional criminal groups that extend some of their activities online.
 - **Aggregate:** These groups are loosely organised and of a temporary nature. Generally, they do not act with a specific purpose. They use digital technologies in an *ad hoc* manner.

TRADITIONAL CRIME AUGMENTED WITH DIGITAL TECHNOLOGY

DOÇ. DR. MURAT VOLKAN DÜLGER

- In considerable number of cases, digital technology is not essential to commit the intended crime, rather it is used to utilise the criminal activity.
 - E.g. Prostitution. As prostitution is illegal, it is not easy to seek out customers. However, the internet has smoothed the way for criminals as exotic ads on web sites allow prostitutes and pimps to advertise prostitution to a large spectrum of potential customers.
 - The use of internet for furtherance prostitution is a “double-edged sword.” Several law enforcement agencies have already executed sting operations centred around these ads: they post their own add, set up an actual meeting and arrest the customers seeking prostitutes .
 - E.g. Online trafficking of the stolen goods. Before online trafficking became widespread, the most practical choice the thieves had was to sell it in their own general region, which actually facilitates law enforcement’s work and help them to catch the thieves by tracing the stolen good. Online sales venues allow thieves in one location to sell their stolen goods across a diverse market space, therefore beclouds tracking the merchandise back to the thieves.

TRADITIONAL CRIME AUGMENTED WITH DIGITAL TECHNOLOGY

- Where digital technology is used to facilitate traditional crimes, **investigators must have a cyber investigation running parallel with the traditional investigation.**
- The digital component of the crime is considered to be an extra burden, however in fact it is an additional opportunity to gather evidence.
 - In practice, there are many instances that the law enforcement agencies have used the internet as part of sting operations.

CYBERCRIMES EXECUTED BY ORGANISED GROUPS

- Purely cyber-based criminal organisations consist of members that are traditional “hackers” who work in unison to commit cybercrimes.
 - Hackers gather and put their resources and skills together for the purpose of executing crimes.
- These cyber gangs consist of groups of highly skilled cyber criminals, therefore they pose a great risk for the digital world as the cumulative efforts of such criminals increases the capabilities of these organisations beyond any individual's.
 - Hence, investigating cybercrimes by cyber gangs require strong coordination, corporation and specialisation *Ibid*, p. 210.

CYBERCRIMES EXECUTED BY ORGANISED GROUPS

DOÇ. DR. MURAT VOLKAN DÜLGER

- Three major types of crimes that committed by these groups:
 - (1) **Identity theft:** Criminal gangs commit this crime on a grand scale and not just steal a few identities. They do not use the stolen information themselves, rather they sell it to anyone who is interested.
 - (2) **Stolen intellectual property:** The most common items are pirated software, video and music. The market for trade secrets and confidential information is relatively small.
 - (3) **Extortion:** More propriate for a group, rather than an individual, due to its complex nature. The most common way to commit this crime is stealing proprietary data and threatening to release it if their demands are not met, or breaching a network and threatening to publish how they did it, hence allowing easy access to other hackers

CYBER TERRORISM

DOÇ. DR. MURAT VOLKAN DÜLGER

CYBER TERRORISM

- «Premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by subnational groups or clandestine agents» (FBI)
- Basically, cyber terrorism is «the use of computer systems to conduct a terrorist attack»

ECONOMIC ATTACKS

- There are numerous ways that a cyber-attack can end up in serious economic damage, such as
 - (i) by destroying data that a company stores,
 - (ii) by causing negative PR,
 - (iii) by compelling a company to pay huge amounts to repair the breach,
 - (iv) through the value of data itself, or
 - (v) by the possibility of a security breach as the presence of this risk itself obliges subjects to purchase various software and hire computer-security professionals in order to preclude any cyber-attacks

ULTRA-SECURE SYSTEMS AND LESS-SENSITIVE SYSTEMS

- It is extremely unlikely that a hacker will crack one of the most secure systems in the world, like the ones at the Department of Defence, Central Intelligence Agency or National Security Agency; however, cracking less-sensitive military systems can cause significant disruption to national defence as well.
- e.g. Suppose that a terrorist cracks a couple of basic logistical operation systems (such as food, mail, fuel, etc.) and he/she notices that cargo planes are being directed a based which is used to transport troops to and from missions; in addition, he/she notices that a massive amount of ammunition and food supplies is synchronically being routed to the same base; also he/she realises that a given unit's all leaves have been cancelled. At that point, it is evident that these troops are preparing to deploy. Our cyber spy would like to disrupt this operation and for that purpose he/she alters the records for the shipment of supplies so that the supplies are delivered two days late and to the wrong location, which undermines the mission of the said troops by interfering with logistics.

INFORMATION WARFARE

DOÇ. DR. MURAT VOLKAN DÜLGER

- Information warfare is «the attempt to manipulate the flow of information in order to alter the outcome of a conflict or a political struggle»
- With the increasing access to information provided by online resources, the number of attempts to spread disinformation to mislead the enemy or to spread propaganda has grown exponentially and such activities have started to become a part of political conflict and open warfare.
- Propaganda tools can also be seemed as a resource.
 - Criminal organisations must disclose some information regarding them, such as names of gang members and information on public gatherings, and this can be an advantage for law enforcement agencies to whom background information is crucial.
- The disinformation campaigns can be also used by law enforcement agencies, and they can utilise the internet to feed misinformation to criminals and terrorists.

CYBER ESPIONAGE

DOÇ. DR. MURAT VOLKAN DÜLGER

- In 2008, the SANS Institute ranked cyber espionage as the third greatest threat on the internet.
- The data stored in computer systems are valuable for two main reasons:
 - (1) creating and analysing the data takes a lot of time and effort,
 - (2) data itself often has intrinsic value.
- Valuable data prompt various recipients, i.e. espionage is utilised by governments, intelligence agencies, international organisations, also by major companies.
 - e.g. CIO Magazine discussed the possibility that the Chinese government is behind many infiltrations, stating that “It has become an article of faith in the information security world that the Chinese government is behind many advanced persistent threats (APTs)—sophisticated, long-term cyber-attacks that target companies for their intellectual property and trade secrets.”
- Cyber espionage must be investigated through following the information as such information can provide clues about who would want that information, which can create a suspect list for the investigators. Combining that information with computer forensic can ease the investigation process.

The slide features a light gray background with decorative circuit-like lines in the corners. The top-left and bottom-left corners have dark blue lines, while the top-right and bottom-right corners have light blue lines. These lines consist of straight segments and small circles, resembling a stylized circuit board or network diagram.

INVESTIGATING ORGANISED CRIME IN THE CYBER SPACE

DOÇ. DR. MURAT VOLKAN DÜLGER

There are two main regulations draw a framework on organised crime and cybercrime:

1. The United Nations Convention Against Transnational Organised Crime ("The Organised Crime Convention")
2. Council of Europe Convention on Cybercrime ("Budapest Convention")

THE ISSUE OF JURISDICTION

DOÇ. DR. MURAT VOLKAN DÜLGER

- Criminal organisations which conduct their activities in the cyber space frequently commit crimes in territories of more than one State.
 - In order to prevent impunity, it is necessary to reduce or eliminate jurisdictional gaps that enable fugitives to find safe havens
- In cases where an organised criminal group is active in several States that may have jurisdiction over the conduct of the group, the international community seeks to ensure that there is a mechanism available for those States to coordinate their efforts.

THE ISSUE OF JURISDICTION

DOÇ. DR. MURAT VOLKAN DÜLGER

- The jurisdiction to prosecute and punish such crimes is addressed in article 15 of the Convention. As per Article 15(1) of the Organized Crime Convention, States parties shall assert jurisdiction over the offences established in accordance with the Convention when they are committed:
 - In their territory ("territoriality principle")
 - On board of a ship flying their flag ("flag principle")
 - On board of an aircraft registered under their laws ("flag principle").
- Article 15(2) also contains a number of optional provisions whereby countries may wish to consider establishing jurisdiction when:
 - The offence is committed against one of their nationals or against a habitual or permanent stateless person resident in their territory. This may also extend to offences against nationals committed abroad. This is called the "passive personality principle".
 - The offence is committed by one of their nationals or by a habitual resident in their territory. This is called the "active personality principle".
 - The offence of participation in an organized criminal group is committed outside their territory with a view to the commission of a serious crime inside their territory. This is called the "protection principle".
 - The offence consists of involvement in money-laundering outside their territory aimed at the laundering of criminal proceeds in their territory.
 - The alleged offender is present in its territory and the State party does not extradite him or her. This is called "aut dedere aut judicare", or "extradite or prosecute principle".

THE ISSUE OF JURISDICTION

- Article 22 of the Budapest Convention requires State parties to adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in therein, when the offence is committed:
 - in its territory; or
 - on board a ship flying the flag of that Party; or
 - on board an aircraft registered under the laws of that Party; or
 - by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

THE ISSUE OF JURISDICTION

- Article 22(5) of the Budapest Convention states that *“When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.”*

THE ISSUE OF JURISDICTION

- Article 15(5) of the Organised Crime Convention provides that *“If a State Party exercising its jurisdiction [h]as been notified, or has otherwise learned, that one or more other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions.”*

INVESTIGATIVE TECHNIQUES AND INTELLIGENCE GATHERING

DOÇ. DR. MURAT VOLKAN DÜLGER

1. It is common for cybercrime to be **transnational** in terms of the physical location of victims, perpetrators, and evidence.
 - It is very likely that in these crimes, the digital evidence required for an investigation may be located in a country, while the offender may be apprehended in another jurisdiction.
 2. Cyber criminals have a variety of **skills** along with their **advanced technical abilities**.
 - It is suggested that these criminals also have skills in linguistics and psychology, and they combine these skills to execute social engineering deception, manipulate decision-making processes and alter perceptions.
 3. A considerable amount of cybercrime is committed through some level of **organisational structure**.
- Thus, compared to traditional criminal offending, cybercrime requires fundamentally different strategic and tactical responses.

INVESTIGATIVE TECHNIQUES AND INTELLIGENCE GATHERING

DOÇ. DR. MURAT VOLKAN DÜLGER

- Effectively investigating organised cybercrime requires special investigative techniques and proactive approaches.
 - Organised cybercrime requires law enforcement agencies to apply technological expertise and deductive reasoning to resolve complex *modus operandi* and substantiate elements of an offense.
 - Law enforcement agencies must be well equipped and competent.
 - While conducting traditional investigation techniques, the specialities of the nature of digital world must be borne in mind.
 - Organised nature of these crimes must be brought into equation in order to ensure success of an investigation.
- Firstly, deductive and inductive reasoning must be employed to establish sequences of events. Then traditional law enforcement techniques including surveillance, interviewing, search and seizure, and formal legal process mechanisms shall be implemented.

INVESTIGATIVE TECHNIQUES AND INTELLIGENCE GATHERING

DOÇ. DR. MURAT VOLKAN DÜLGER

- Article 20(1) titled “Special Investigative Techniques” of the Organised Crime Convention expresses that *“If permitted by the basic principles of its domestic legal system, each State Party shall, within its possibilities and under the conditions prescribed by its domestic law, take the necessary measures to allow for the appropriate use of controlled delivery and, where it deems appropriate, for the use of other special investigative techniques, such as electronic or other forms of surveillance and undercover operations, by its competent authorities in its territory for the purpose of effectively combating organized crime.”*
 - Undoubtedly using covert human intelligence sources, i.e. undercover agents have an important role for the proactive approach pursuant thereto.



THANK YOU VERY MUCH...

For details and related articles and presentations:
<http://aydin.academia.edu/DoçDrMuratVolkanDülger>