Cybercrime : Malaysia

By

DSP Mahfuz Bin Dato' Ab. Majid
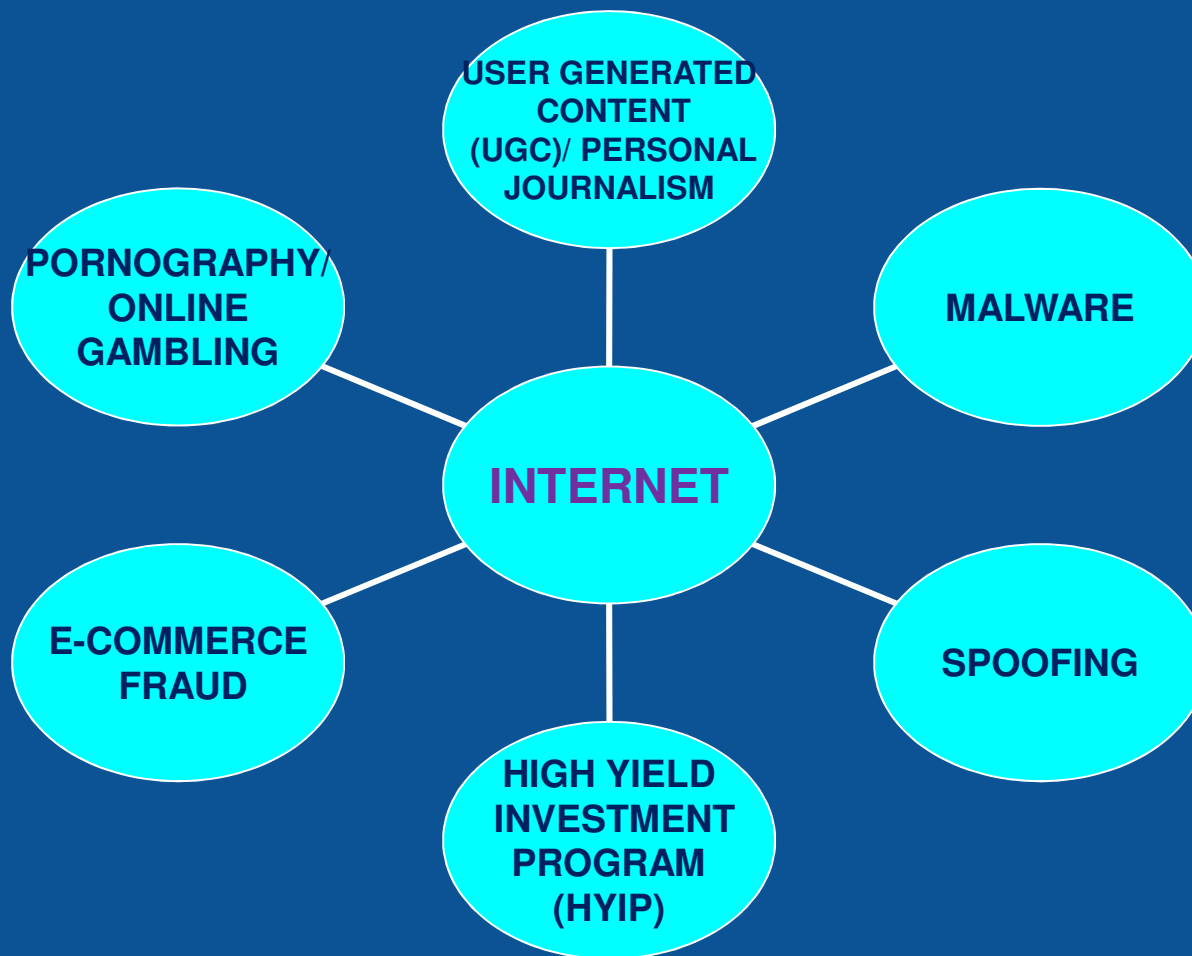
Royal Malaysia Police

ICT Development

- The ICT development within this region has been rapid since more than 3 decades ago.

- With the launching of the MSC in 1996, these cyber related development has transformed Malaysia into a regional ICT hub.

- Government and commercial portals offering everything from administrative information, interactive and online communications besides financial transactions have sprung up to cater to almost very need.

- Following closely behind rapid ICT developments are related risks that have emerged and evolved in almost all aspects of life posing a real threat to country's well-being.

- These cyber-related risks have posed serious challenges to any government and in particular to the law enforcement agency in keeping law and order.

- Rapid and in some cases, uncontrolled ICT development have created challenges in the form of loopholes in current laws, economic development, political stability and social/ racial well-being.

- The new millennium law enforcement agency is now faced with the task of enforcing law in cyberspace that transcends borders and raises issues of jurisdiction.

CYBERCRIME

- Cybercrime has surpassed drug trafficking as the most lucrative crime.

- Almost anybody who is an active computer/ online user would have been a cybercrime victim, and in most cases too its perpetrators.

- The younger generation are the most vurnerable.

- Use of technology to cheat, harass, disseminate false information.

- 70 % of commercial crime cases now can be categorised as cybercrime cases.

MALAYSIAN TECHNOLOGY/ COMPUTER CRIME CASES

- INTERNET
  - USER GENERATED CONTENT (UGC)/ PERSONAL JOURNALISM
  - PORNOGRAPHY/ ONLINE GAMBLING
  - MALWARE
  - E-COMMERCE FRAUD
  - SPOOFING
  - HIGH YIELD INVESTMENT PROGRAM (HYIP)

CYBERLAWS OF MALAYSIA

1. COMPUTER CRIME ACT 1997
2. COMMUNICATIONS AND MULTIMEDIA ACT 1998 (CMA)
3. MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION ACT 1998
4. DIGITAL SIGNATURE ACT 1997
5. COPYRIGHT ACT (AMENDMENT) 1997
6. TELEMEDICINE ACT 1997
7. OPTICAL DISC ACT 2000
8. ELECTRONIC TRANSACTIONS ACT 2006

ROYAL MALAYSIA POLICE

MALAYSIA CYBERCRIME CASES

YEAR	TOTAL CASES	LOSSES (RM MILLION)
2007	1139	11.4
2008	1821	12.9
2009	3863	22.3
2010	6167	63.0
2011	6586	80.5
2012	4738	96.1

TOP 3 NUMBER OF CASES:

1. E-COMMERCE FRAUD- ONLINE PURCHASE
2. PARCEL SCAM
3. VOIP SCAM- CROSS BORDER SYNDICATES

ROYAL MALAYSIA POLICE

Reported Incidents based on General Incident Classification Statistics 2012
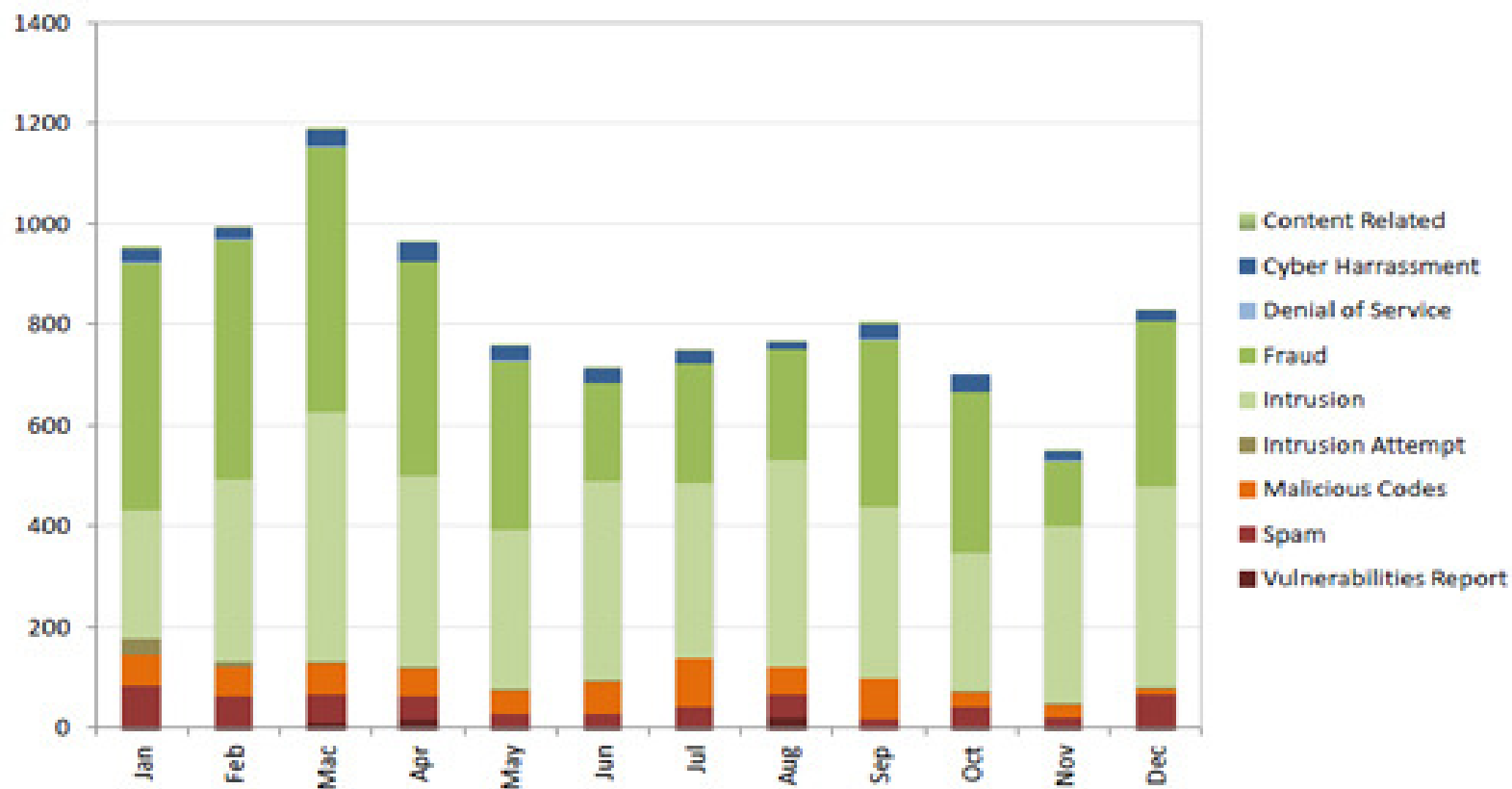
Cyber Threats

- **Economy**

  Online fraud and threats can undermine any efforts to promote economic development and stability. Being key in promoting investment opportunities and a healthy business environment, economic stability that is exposed to constant and serious online threat that can jeopardise years of any development effort.

  - **Online Fraud.**

    – Fraud cases can be propagated from a few countries and comprising of groups of individuals. Eg. African Advance Fee Fraud scams, VOIP Spoofing Scams and SMS Scams.

  - **Phishing.**

    – The collection of personal data through illegal means are now done internationally by electronic crime syndicates and in most cases, data are then used in collaboration with local syndicates to fully utilise or take advantage for the purpose of illegal gains.

  - **User Content Issues.**

    – Blogs and other online publications offers a convenient platform for the purpose of publication of opinion and uncensored news but unfortunately open to abuse against individuals, organizations and even the government.

- **Cross Border Intellectual Property and Licensing Issues.**

  - The challenge of controlling crossborder transfer of intellectual property especially of illegal material under Malaysian law. Similarly, the subscription by Malaysians to sites considered illegal under Malaysian law such as pornography and gambling raises concerns over the control illicit material accessible to Malaysians besides control on outflow of funds.

- **Information Theft.**

  - Corporate or business data being stolen for the benefit of competitors, whether by current employees or through the use of technology such as Malwares or now better known as Crimeware. Crime tools are now available online making amateurs able to perform online tasks such as to spoof websites or hack into systems easily unlike 5 or 10 years ago when it could only be performed by trained individuals.

- **Social/ Racial Balance**
  - Unlimited and unrestricted online social interaction have spawned serious underlying issues .
  - Most serious will be the use of fake online identities which more often than not leads to cheating cases.
  - Exposure to false and malicious information that is spread via the internet and SMS have led to racial problems.
  - The attacks have not only targeted the government and political parties but individuals and organisations.
- **Terrorism**
  - As with other online criminal networks, the threat of cyber terrorism cannot be taken likely whether in the form of direct attacks against Critical National ICT Infrastructures, the spread of political or militant propaganda and even recruitment of potential members.
  - Extremist groups, separatist forces, advocates of ideas.
  - RMP have over the years monitored closely the online development particularly in relation to the spread of online propaganda. To date, more than 15 websites that are suspected have been taken offline or blocked with the cooperation of the Malaysian Communication Multimedia Commission.

Issues

- Close analysis of present day cyber attacks against organisations are mainly from:

  - within/ insiders

  - via insiders

  - introduction of malwares

  - external attacks

CURRENT CHALLENGES IN CYBERCRIME INVESTIGATION

- Mobility of devices proving to be biggest challenge to law enforcement in tracking and analysing equipment.

- Introduction of new technologies and economic innovations. Ensuring adequate analytical and technical capabilities for law enforcement .

- Maintaining a comprehensive and relevant legal framework.

- Working in a borderless environment with laws of multiple jurisdictions. Issue of differences in national priorities.

- Implementing information security practices and raising awareness.

- **ICT Awareness**

  – Online Content Awareness
  – Security Awareness: Password, IDS, Anti Viruses etc.
  – ICT Onsite security issues. Security Processes

OUR RESPONSE

- Review of current laws
  - Computer Crime Act
  - Evidence Act, Penal Code etc
- Inter-agency task force (Local)
- Participation in Awareness campaigns
- Police Cyber Investigation Response Centre (PCIRC)
  - Supported by the Mobile Intelligence System (MIS)
- Departmental Training
  - Cybercrime Investigations, VOIP, Wireless, Multimedia & Network Forensics.
- Other Agency courses
  - Cyberlaw & cybercrime courses
  - Ilea (Bangkok), PTI (Bangkok/ Manila), JCLEC (Jakarta) Interpol.
  - Microsoft, Cisco
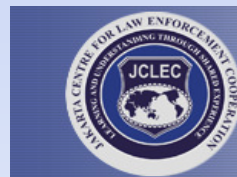
ROYAL MALAYSIA POLICE

Sign Up **Facebook helps you connect and share with the people in your life.**

Polis Diraja Malaysia (Royal Malaysia Police) 👍 Like

Government Organization · Kuala Lumpur, Malaysia

Similar Facebook Pages

Environmental Council

AFN Livorno

Bordo Bereliler Sat Ve Sa Komandolar TÜRKİYE

▼   More

Wall

Polis Diraja Malaysia (Royal Malaysia Police)

BELUM ADA PERMOHONAN PERMIT GUNA STADIUM : Melalui sidang media yang diadakan di Bukit Aman petang semalam, Dato' Sri Khalid bin Abu Bakar, Timbalan Ketua Polis Negara berkata, PDRM menjunjung kasih titah Seri Paduka Baginda Yang di-Pertuan Agong mengenai pembatalan perarakan atau perhimpunan jalanan yang dicadangkan pada 9 Julai ini....

See More

Wall Photos

🖼 6 hours ago · Like · Comment

👍 Farhan Simiele Trw, Pitih Skeleng, Le Pe La and 151 others like this.

💬 View all 63 comments

Facebook Rasmi Polis Diraja Malaysia

KECEMASAN SILA HUBUNGI :
03-22663333
03-20319999
mcc@rmp.gov.my
www.rmp.gov.my

💬 **Wall**
📄 Info
🖼 Photos
📄 Notes
💬 Discussions
🔗 Links

Polis Diraja Malaysia (Royal Malaysia Police)

Program PDRM bersama Pelanggan

Pelaksanaan program 'PDRM Bersama Pelanggan' adalah sebagai salah satu inisiatif ke arah mencapai objektif National Key Performance Indicator (NKPI) iaitu untuk Meningkatkan Kepuasan Masyarakat Terhadap Perkhidmatan Polis

- **Equipment/ Application procurement**
  - E-mail tracking system, Investigative Toolkits, formation of forensic 'First Responder Team'
- **Upgrading of Forensics capabilities**
  - Transition from offline data recovery analysis to online/ realtime analysis.
  - Introduction of *First Responder* team
- **Inter agency/ international cooperation**
  - CTINS, 24 hour Point Of Contact Network.
  - Interpol, Europol, Virtual Global Taskforce (VGT)

ROYAL MALAYSIA POLICE

Questions?