SUBMISSION NO. 21

Inquiry into Cyber Crime and its impact on consumers

Rapport written by the INTERPOL's Financial and High Tech Crime Sub-directorate
June 2009

I INTRODUCTION: Internet, a new global scenario

1. Whenever we talk or hear about internet, different scenarios may arise:

   a. How technology has made an impact on human behavior in such a short period of time, changing activities that used to require peoples "real presence" into an only "virtual presence" required that allows them to can be done from an office, home or even abroad, or how society has increased its productivity and how entities could reduce costs by hiring people who can work from their own homes, for instance.

   b. On the other hand, we hear on the news about people "hacking" different web sites, or concepts like a DOS attack, or trojan, malware which probably don't mean much to society, but still can be very harmful for all of them; and sometimes we hear about people having their bank account empty, due their payment card was "skimmed".

   c. Even though we can learn on the news that someone was killed or had a car accident, this doesn't mean that we won't go out nor will not drive our car. Making an analogy, though undesirable events may occurr while using internet, we still use it, but not thinking on the **risk** we are taking.

II RISK AND UNCERTAINTY

1. Whenever we take the decission of making a bank transaction over the INTERNET, are we making a rational decission? which should mean that we are aware of all risks involved? Are we completely unaware of the risks related? Or is it just that we don't think that we could be scamed?

2. Before we continue, let's clarify a couple of concepts. Do risk and uncertainty mean the same?

   According to Oxford English Dictionary, **uncertain** means ***"not known, reliable, or definite"***. It could be consider as "random walk".

   Risk? The same dictionary states that is ***"a situation involving exposure to danger. 2 the possibility that something unpleasant will happen"***.

To be more accurate, possibility does not define well enough the meaning of risk. If we call it ***probability,*** it should be more accurate and suitable. Therefore the difference, it seems clear: **an event can be possible or not; but how probable it becomes makes a complete different concept.**

3. But based on what we determine the probability of an event? Is past the best predictor we have?

So, It is related with the probability of occurrency of an event. But based on what? Is the past the best predictor we have?

Certainly not but we don't have much left.

According to Markov's chain model[1], we could think that crime on the internet (and most of crimes) could be considered as a specific stochastic process, where future states are independent of past states. So a future state depends on the present state, and it will be reached through a probabilistic process instead of a deterministic one.

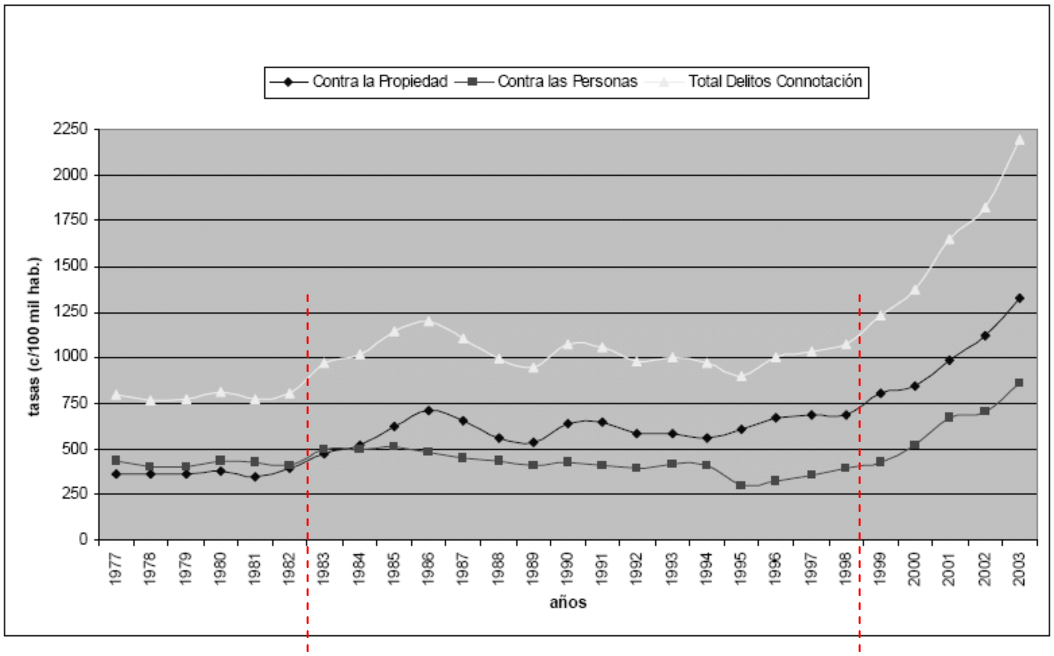
$$\boxed{\Pr (X_{n+1} = x_{n+1} \mid X_1 = x_1, X_2 = x_2,\ldots, X_n = x_n) = \Pr (X_{n+1} = x_{n+1} \mid X_n = x_n)}$$

Just a question then: can criminal behavior be predicted? We could tell WHAT they're going to do: is very likely that criminals will commit crimes within their specialities. But we still need to know WHERE and WHEN if we isolate criminals patterns (their signature in any Crime Scene), we could set a distribution of probabilities to answer these questions or is it completely RANDOM? It could be random **but** within a trend and within a range.

[1] http://en.wikipedia.org/wiki/Transition_probabilities

III CRIME AND ECONOMY

Take a minute and review this information from a research done by a member country on major crimes from 1977 until 2003.



http://www.seguridadpublica.gov.cl/filesapp/diagnostico_seguridad_ciudadana_chile.pdf

Even though the study didn't mention it, it's interesting that until 1982, we could see an stationary time serie, but then we see an increasing trend. Then again a stationary serie from 1988 until 1998, when again turns into an increasing trend. An important question that we could ask ourselves is what happened that an stationary time series changed? We don't have enough information to answer that, but coincidentally those two years the world was hit by economic crisis. So are crime and economic cicles related?

IV RISK APPROACH

1. We must remind that in any area, such as finance, there are many different risks that managers have to deal with, but the first step it was to identified them:

   - Market risk
   - Credit risk
   - Sistemic risk
   - Liquidity risk
   - Operational risk
   - Bankrupcy risk, among others.

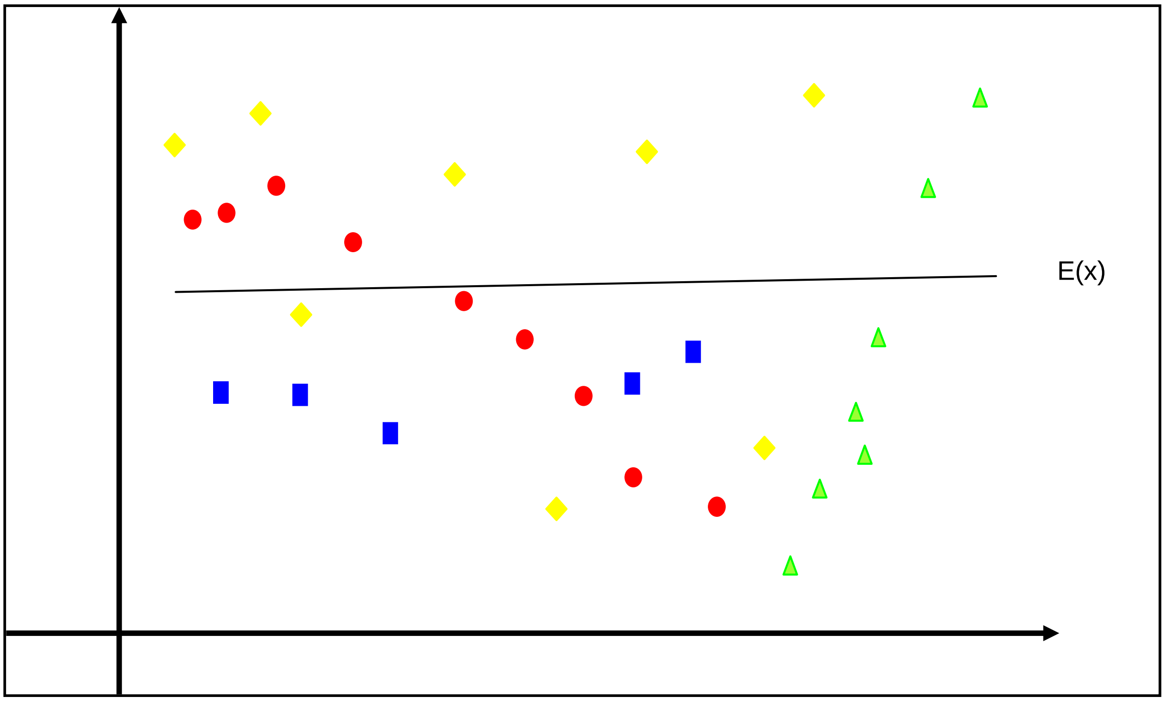
Then a risk must be measured and then see if it can be minimized, tranfered or deleted.

2. In order to understand this new approach to crime, we will use payment card fraud as an example.

3. We all know what are the parties involved in a single ATM transaction, event that it could happen anywhere in the world.

    a. A customer
    b. An ATM
    c. A Payment Card
    d. A Bank that issued that card
    e. Communication devices (that links the ATM with the bank)
    f. Outsourced workers
    g. Etc.

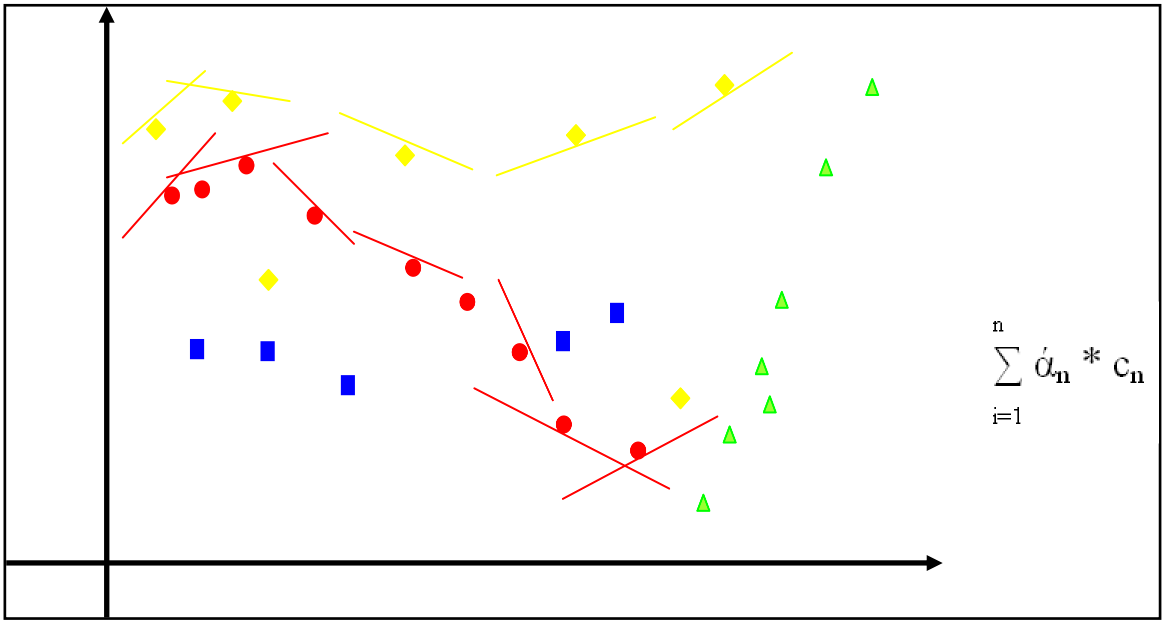
    Each one of the parties above mentioned, could be consider as risk scenarios. Considering that there are different types of risks, it is difficult to assume that we will find an only one solution that fits all. If we consider this alleged solution as the average, we could draw the following chart where different risks are in different colours and the line in the middle could be our average projected in the future.



INTERPOL, FHT 2009

In this case average or mean does not represent much in long term.

4. If we isolate cases, and separate them according to certain parameters (patterns), we could find new risks or even its causes.



INTERPOL, FHT 2009

So an approach that understands and foreseens this phenomenon should allow analysts to isolate different scenarios involved, and contribute with solutions that could lead to tackle as many risks found, having the oportunity to either predict future scenarios (proactive) or increase its reaction capabilities. Actually the summatory of many tangents to each individual risk profile will end up being the shape for that original curve or function.

We should remember that it doesn’t matter how secure a payment card is if we still have customers that don’t know how to use it; or don’t take security measures when entering their PIN; or answer e-mails sending out their information, including bank account, PAN and PIN, plus expiry date and security code. Or even if some countries have implemented a CHIP & PIN solution, building a more secure payment card, information on the magnetic stripe can still be taken with a skimming device, then pass it to a white plastic card, and withdraw money from ATMs in countries where this type of solution has not yet been implemented; this information could be sent overseas by e-mail and we could have a skimmed payment card on the other side of the world within seconds and ready to “operate”.

Another novel way of ATM skimming, or hacking would be a better word for that, where Diebold ATMs[2] were attacked by fraudsters using sophisticated virus, which was informed to us by a member country. They stated that ***"this malicious code allows PIN PAD software of Diebold's ATM to decode PIN and stores it on hard disc along with data from magnetic stripe. Than fraudsters, use special chip card which instructs infected ATM to print compromised data (including PIN) on the regular ATM slip. As criminals are using mules to retrieve data from ATMs, information printed on the slip is encrypted making it useless for the mule and then decrypted by criminals for further use.***

Based on the information provided by impacted local banks in most of the cases, a virus was installed through the USB and administrator level system access while the ATMs were opened using original key which can lead to suspicion of internal fraud (but not necessarily). We have also seen cases where a whole was drilled in the ATM face. Operating system in all the cases was Windows XP.

In addition to that one of local banks informed that at the end of Feb'09 fraudsters developed the virus which makes Diebold ATM give all cash from any given ATM".

V INTERPOL's EFFORTS TO TACKLE E-CRIME

1. There are working parties designed to reflect regional expertise and exist in all INTERPOL regions. All working parties are in different stages of development. It should be noted that the work done by the working parties is not Interpol's only contribution to combating ITC, but it certainly represents the most noteworthy contribution to date. As an example, Interpol Working Party on IT Crime Europe, formed in 1990, it meets three times a year. In 2009 the Interpol General Secretariat will host 3 meetings of the working party. It is currently represented by members from Austria, Belgium, Denmark, Finland, France, Germany, Italy, Netherlands, Norway, Portugal, Sweden, Switzerland, Spain, and United Kingdom. Among its achievements:

   a. The **Manual and the Best Practice Guide** for the experienced investigator has become a very practical tool, which is continually updated.

   b. **First Responders Project** (in close co-operation with the Australian Federal Police)**:** instructions on how to handle digital evidence. It is as short as possible without warnings or disclaimers.

   c. **Counter forensics Project:** questionnaire surveying counter forensic methods.

   d. **Network Group:** a questionaire regarding current status of IT crimes in member countries.

[2] http://www.diebold.com/solutions/atms/opteva/html/

e. **Botnet Follow-up project:** The project team created and updated the chapters of the Botnet Follow-up document about newer types of botnets and also Updated the training manual with new techniques and new trends on Botnets & Malware.

2. During INTERPOL's 77th General Assembly held in St. Petersburg (October 2008), the General Assembly overwhelmingly approved INTERPOL's Global Security Initiative (GSI). GSI is a comprehensive, strategic effort, capitalizing on INTERPOL's unique position as the world's largest multilateral law enforcement entity, to help countries address 21st century global crime challenges.The GSI has five core components: Global Security, Secure Global Infrastructure, Global Law Enforcement Capacity, Strategic Global Partnerships, and Innovation. While the Cyber Forensics Unit is recognized as a critical first step, the GSI team has identified a broad and compelling need for a dedicated Cybercrime Initiative to expand INTERPOL's current cyber security efforts.

3. This year INTERPOL and University College Dublin (UCD) have launched a specialist training initiative that will help establish a recognised international standard for digital forensics and cybercrime investigations. The agreement will provide a framework to implement training as well as academic exchanges to jointly promote law enforcement e-crime investigation expertise and foster computer forensic incident response capability throughout INTERPOL's 187 member countries[3].

4. INTERPOL initiative with Microsoft aims to raise global standards against cybercrime through strategic partnership with IT sector. Under this agreement, Microsoft made available to INTERPOL's 187 member countries its Computer Online Forensic Evidence Extractor (COFEE) software tool to aid law enforcement investigators in incident response investigations access live computer system data[4].

5. INTERPOL is committed to raising global standards in the fight against IT crime, and these agreement will see law enforcement officers from around the world benefit from specialist training in a range of areas including: preserving electronic evidence, enhancing investigation techniques for online crime, capturing evidence of covert activity and managing intelligence-led operations - all essential areas to 21st century e-crime investigations.

[3] http://www.ucd.ie/news/2009/06JUN09/050609_interpol.html

[4] http://www.interpol.int/public/ICPO/PressReleases/PR2009/PR200937.asp

INTERPOL IPSG has developped five focus areas for the field of cyber crime investigations:

Focus Area One: Computer Forensics, Analysis of Evidence, and Online Investigations

Computer Forensics & Analysis of Evidence

- Provide core team with technical equipment and subject matter expertise
- Establish case officers to liaise with associated crime verticals

Online Monitoring & Investigations

- Establish common protocols for monitoring
- Provide direct support to member countries
- Pre-emptively alert member countries of cyber threats
- Serve as a trusted broker to expedite sensitive information exchange

Focus Area 2 – Training, Capacity Building, and In-House Support

Focus Area 2 will expand cyber-based training initiatives, enhance member country capabilities, expand regional partnerships, and provide support for internally-oriented elements of the Centre.

- ***Training & Capacity Building***
  - Establish critical mass of accredited trainers
  - Provide supplement equipment resources on-the-ground
  - Promote remote e-learning opportunities
  - Advise private industry on how to properly connect with law enforcement on select cyber incidents
  - Promote regional partnerships to scale / replicate internal training efforts
  - Subsidize training for less developed countries
  - Set initial standards and/or guidelines in cooperation with Training Office
- ***In-House Support***
  - Author basic principles for first responders
  - Develop common techniques to ensure anonymous network monitoring
  - Implement professional development to keep pace with technological change

Focus Area 3 – Cyber Domain Situational Awareness

Focus Area 3 will establish a common operating picture (both internal and external) for emerging threats to global networks while leveraging INTERPOL's existing communications and data exchange infrastructure.

- **External Component**
- Connect domestic cybercrime units to I-24/7 network
- Establish incoming link to private Secure Operating Centres to eliminate prevailing disconnect between responding to an incident (temporary patch) and investigating an incident (long-term prevention)
- Enable rapid-action response (see potential legal constraint)
- Institute early warning system (e.g., purple notices)
- Catalogue incoming data from the private sector

- **Internal Component**
- Match compatible databases and aggregate trends observed in crime verticals alongside general cyber trends
- De-conflict "blue-on-blue" operations

Focus Area 4 – Build Public-Private Partnerships

Focus Area 4 will encourage INTERPOL to invest energy in organizations that sit at the nexus between policy and practice, where it can effectively enhance its position and reputation as the global authority on cybercrime.

- *Academia*
    - Construct "cloud" of cyber subject matter experts (networked think tank model)
- *International Organizations*
    - Seed select organizations with presence to establish INTERPOL as the law enforcement authority in cybercrime (e.g., IMPACT)
    - Continue to influence the policy landscape and forthcoming legislative proposals related to cyber (CoE)
    - Expand focus to other regional groups
- *Private Organizations*
    - Establish data link with Internet Service Providers / DNS Registry Systems
    - Establish data link with Banking and Financial System
    - Specialized law enforcement data (e.g., Cymru)
    - Computer Emergency Response Teams
    - SANS Institute (Internet Storm Centre)

Focus Area 5 – Review and Evaluate the Impact of Emerging Technology on Law Enforcement

Focus Area 5 will attempt to mitigate the gap that has grown between the emerging threat and countervailing solutions by investing time in understanding solutions before they come to market.

- Understand emerging technology in the context of its impact on law enforcement (advanced previews)
- Evaluate and endorse hardware / software tools to ensure a progressive baseline for IT security
- Survey development efforts within the law enforcement community and publish new or innovative investigative techniques
- Continue to monitor and advise on malicious toolsets and techniques that are emerging from the hacker community

VI FINAL WORDS

As we accelerate into the 21st century, cybercrime is increasingly recognized as a dangerous and persistent threat to international security, manifesting itself in countless ways that directly impact citizens, business interests, and governments alike. It is a global phenomenon that threatens our critical infrastructures such as nuclear facilities, transportation systems, communications networks, and public utilities. Cybercrime includes not only bank fraud and identity theft, but encompasses all aspects of illicit behavior that can be facilitated through the Internet, from child exploitation to terrorism.

To tackle e-crime requires:

- Sharing information: risk assessment.
- Determine new procedures, in order to minimize, transfer or eliminte risks assessed.
- Due to globalization (also of criminal organizations and the usage of technologies), establishing an standardizing laws around the world, and for law enforcement agencies setting up best practices manual gathered from international experience, should be a step forward where an evidence anywhere can be use on court safely.

- This virtuosity ring against crime requires permanent efforts in sharing information, coordination and assessing of the current local and international trends, in order to have predicting skills of emerging risks.
- We could have congressmen, police officers, prosecutors, banking industry and private sector in general, education system (enhancing values) and developing new training capabilities within law enforcement, national authorities and international efforts all alligned to achieve the same goal:

Representatives from government, law enforcement, and private industry must work together to consolidate and coordinate ongoing efforts in order to present an effective defense against emerging cyber threats. INTERPOL's position as a sophisticated, global law enforcement entity makes it uniquely positioned to effectively address crucial aspects of this accelerating transnational menace where combating cybercrime is an urgent global need.

For further details please feel free to contact Mr Bernhard Otupal, Assistant Director of INTERPOL's Financial and High Tech Crime Sub-Directorate, or Mr Jaime Ansieta, Criminal Intelligence Officer.

- - - - - - - -