ELECTRONIC CRIME UNIT

Brigadier NT Pieterse
Section Head: Electronic Crime Unit (ECU)
Directorate for Priority Crime Investigation
Commercial Crime
South African Police Service
pietersent@saps.gov.za
ecu@saps.org.za
082 463 7227

NSTF Discussion Forum// ICT Security and Privacy
Emperors Palace 15 May 2015
Establishment of Specialised capacity

The Directorate for Priority Crime Investigation have identified cybercrime, which unique characteristics resemble elements of organised crime committed nationally and cross border, as a high priority, specifically in relation to the broader financial platform

The establishment of specialised capacity within the Directorate to address the occurrence of the cyber threat to the South African economy and democracy have thus been a high priority, resulting in the creation of the Electronic Crime Unit within the Directorate’s Commercial Crime environment
Mandate of Directorate

To prevent/combat/investigate National Priority Offences

National Priority Offences Section 17A of SA Police Service Act

Organised Crime

Crime that requires prevention/investigation

Crime that requires specialized skills

Cybercrime varies from relative insignificant transgressions to transnational organised crime

Organised crime syndicates utilize proceeds of cybercrime to finance other organised criminal operations

Cybercrime negatively impacts on the economy of all countries in the world/ adversely affects public administration/trust in Information Communication
Structures within Directorate

**ELECTRONIC CRIME UNIT (ECU)**

Nationally based Unit responsible for the prevention/combating/investigation of cyber related crime on the broader financial platform through an integrated multi disciplinary approach

**DIGITAL FORENSIC LABORATORY (DFL)**

DFL responsible for the acquisition/analysis of technological evidential instruments/forensic peripherals in relation to the broader organised crime platform
The JCPS Cluster signed on 24 October 2010, the JCPS Delivery Agreement, relating to

Outcome 3: “All People in South Africa Are and Feel Safe” This Outcome focuses on certain areas and activities, clustered around specific Outputs, where interventions will make a substantial and a positive impact on the safety of the people of South Africa

Output 7: requires the development/implementation of a Cyber-security Policy/the development of capacity to combat/investigate cybercrime

In line herewith, the Cabinet approved the National Cyber-security Policy Framework (NCPF) for South Africa
The NCPF is intended to implement an all encompassing approach pertaining to all the role players (State/public/private sector/civil society/special interest groups) in relation to Cyber-security

In terms of the NCPF, South African Police Service shall be responsible for the prevention/investigation /combating of cybercrime in the Republic, which includes:

- Development of cybercrime policies / strategies
- Collaboration with appropriate stakeholders
- Development /maintenance of enforcement capabilities
- Improve basic understanding of cybercrime within SAPS

The National Security Strategy-approved in December 2013 by Cabinet emphasized cybercrime as a priority threat to national security that NEEDS TO BE ADDRESSED THROUGH A HOLISTIC, COMPREHENSIVE CYBERCRIME POLICY
South African Police Service Strategic Plan

“...Directorate for Priority Crimes Investigation (DPCI) is one of the key investigative organs in the SAPS that require the necessary capacity and expertise in order to give full effect to its mandate...This Directorate represents a specialised investigative capacity within the SAPS whose focus is on crimes that are a national priority such as serious economic crime, with a KEY CONSIDERATION being the COMBATING OF CYBERCRIME...”
ENTER THE ELECTRONIC CRIME UNIT
Case study ABC BANK

ABC bank primarily host clients from the previously disadvantaged communities/only deals with savings accounts/small investment accounts.

ABC Offices nationally act as branches for ABC bank.

ABC bank account operates in same manner as an “ordinary” bank account. Some clients prefer to still make use of a ABCbank book linked to their account, whilst other customers (account holders) prefer a ABC bank card.

Card be utilized as a debit card/be presented at stores for payment on purchases instead of cash.
On 3 January 2012 ABC bank established R42 782 500-00 fraudulently deposited into 103 ABC bank customer beneficiary accounts

R30 882 800-00 unlawfully withdrawn during 5 437 ATM’s transactions

Apparent that the cyber heist committed in a sophisticated/organised fashion, by a group of persons/syndicate/enterprise, acting in the execution or furtherance of a common purpose or conspiracy over a period of time

ABC Bank normal ATM daily withdrawal limit is set at R1 000-00, yet increased to R500 000,00
COMPARE 45m USD “Yonkers”/ABC bank

Very good example how complex (yet simple) organised crime targeting electronic banking products has become

Raising of daily limits-similar to ABC bank

Use of ICT infrastructure to enable large organised crime attacks across borders (transnational)

ATM as preferred cash out method (also case in SA)

Decentralized attack-cash payout decentralised (as many as 24 countries involved)

Data theft from processing centres (huge risk-not strictly regulated)
It was a happy New Year’s Day for gang who pulled off . . .

R42m ABC bank heist

NIA called in to probe hi-tech hacking

WERNER SWART and MZILIKAZI WA AFRIKA
ABRAZEN
A hi-tech heist over three days has left XXXbank, part of the South African XXX Office, out of pocket to the tune of R42-million. Now the National Intelligence Agency (NIA) and the police have launched a high-level probe. The theft raises concerns that the security network of the bank — which holds about R4-billion in deposits and through which millions of rands in social grants move each month — is far too fragile.

The 72-hour heist comes as ABCbank seeks to become a separate entity and get a full banking licence from the Reserve Bank to allow it to compete with commercial banks while still being state-owned. The Sunday Times can reveal that what is thought to be a cybercrime syndicate with knowledge of the XX office’s IT systems launched its operation on New Year’s Day.
Challenge facing law enforcement in relation to the cyber crime phenomenon is in essence a faceless one

Extremely complex to determine the true identity of a cyber crime perpetrator/identify the geographical location from where the cyber criminal operates/predict a pattern of behavior in relation to the unlawful cyber activities

Cross-national nature of most computer related crimes have rendered many time honored methods of policing, both domestically and in cross border situations ineffective, even in advanced nations, while the “digital divide” provides “safe havens” for cyber criminals
INVESTIGATIVE RESULT

February 2012 – Mr Bxxx Mxxx Txxx arrested - On 22 February 2012 sentenced 25 years imprisonment

February 2012 - Mr Dxxx Mxxx Mxxx arrested - On 1 March 2012 sentenced 15 years imprisonment

February 2012 Mr Txxx Lxxx Dxxx Mxxx
During March 2012 sentenced 15 years imprisonment

On 19 April 2012 the investigating team achieved a major breakthrough in the investigation with arrest of Mr Kxxx Kxxx

During June 2014- sting operation- ABC bank- R30 000 000, 00 outstanding target arrested –section 252 CPA operation
INVESTIGATIVE RESULT

Desired outcome: To disrupt the identified Transnational mass marketing/ credit card/ romance –reshipping phenomenon Organised Criminal Business System

Result:

Positively identified 200 members of the Transnational Organised Crime Syndicate operating in a number of countries

First Leg of Scams-R-Us  
May 2014- Simultaneous take-down operation in SA/US/Canada (INTERPOL)- search seizure/arrests/forfeiture accused in SA extraditions authorized

Second Leg of Scams-R-Us  
December 2014- Simultaneous search seizure/arrests/ASSET FORFEITURE operation- UK Law enforcement arrest identified main target Heathrow on route to SA- seize in an abundance of digital evidence

Strategic outcome in successfully eradicating cyber crime could certainly be entrenched in the knowledge that destroying computer generated information turns out to be surprisingly difficult

Fossilization of deleted information means that a forensic footprint could well exist

There is a positive aspect to the increasing use of technology by criminals in that the involvement of computers in crime has resulted in an abundance of digital evidence that can be used to apprehend and prosecute offenders
<table>
<thead>
<tr>
<th>MAJOR INVESTIGATION/NATIONAL PROGRAM</th>
<th>PHENOMENON/THREAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC bank</td>
<td>Cyber Crime Intrusion (CCI)</td>
</tr>
<tr>
<td>Scams-R-Us</td>
<td>Transnational Hacking/Mass Marketing Fraud</td>
</tr>
<tr>
<td>F*** F**</td>
<td>Credit/Debit Card and Card not present Fraud</td>
</tr>
<tr>
<td>Eskom</td>
<td>Cyber Crime Intrusion (CCI)</td>
</tr>
<tr>
<td>V***/ N******</td>
<td>Cyber Crime Intrusion (CCI)</td>
</tr>
<tr>
<td>S**********</td>
<td>High Tech Skimming Fraud</td>
</tr>
<tr>
<td>I**********</td>
<td>High Tech Skimming Fraud</td>
</tr>
<tr>
<td>G**********</td>
<td>Handheld Skimming Fraud</td>
</tr>
<tr>
<td>I********** E****** C********** (***</td>
<td>Cyber Crime Intrusion (CCI)</td>
</tr>
<tr>
<td>Gautrain Management Agency</td>
<td>Cyber Crime Intrusion (CCI)</td>
</tr>
<tr>
<td>G**********</td>
<td>Sim Swap/Phishing</td>
</tr>
<tr>
<td>RTMC- Road Traffic Management Corporation</td>
<td>Cyber Crime Intrusion (CCI)</td>
</tr>
<tr>
<td>Mini Cooper</td>
<td>Identity Theft /Fraud, Sim Swop/Phishing</td>
</tr>
<tr>
<td>No.11</td>
<td>Identity Theft /Fraud, Sim Swop/Phishing</td>
</tr>
<tr>
<td>M*****</td>
<td>Asset Base Fraud-Home Loan Application</td>
</tr>
<tr>
<td>A**********</td>
<td>Asset Based Fraud- Home Loan Application</td>
</tr>
<tr>
<td>R**********</td>
<td>Asset Based Fraud- Vehicle Application</td>
</tr>
<tr>
<td>W**********</td>
<td>Asset Based Fraud- Home Loan Application</td>
</tr>
<tr>
<td>D**</td>
<td>Cyber Crime Intrusion (CCI)</td>
</tr>
</tbody>
</table>
CAPUT LUPINUM
WE EVEN HAVE OUR OWN JASON BOURNE AKA MATT DAMON
CYBERCRIME ESTIMATE

Shortage of skilled investigators increases our vulnerability
Cyber criminals exploit vulnerabilities
Lack of cyber security awareness heightens vulnerability
Lack of cooperation/collaboration between public/private sector

We will remain vulnerable to cybercrime
At least until National Cyber-Security Policy Framework (NCPF) fully implemented
ACTIONPLAN

Develop effective communication strategy to heighten awareness of cyber security/cybercrime

Finalize/implement the Cyber-security and related matters Bill

Strengthen early warning/monitoring mechanism to protect cyber infrastructure/systems-critical information infrastructure

Conduct simulation exercises to identify/address cyber vulnerabilities

Build capacity to detect/prosecute cybercrime
A futuristic approach in addressing cybercrime
Maintain and further develop enforcement capabilities

Create “on-line” operational investigative mechanism capacity in order to expose (detect/investigate) cybercrime criminal business enterprise structures, specifically in relation to (but not limited to) identified phenomenon “on-line” scams relating to mass marketing fraud/advance fee fraud/data and “crypto-locker” intrusion investigations, and misrepresentations made by cyber perpetrators via the internet (be extended to Organised Crime and Corruption platform)

Establishment “workstation” infrastructure- inclusive of physical infrastructure and software design/maintenance/hosting associated with foreseen ICT infrastructure

Training of identified “on-line” DPCI investigators

Establishment of internal processes/ procedures/ investigative methodologies/best practices in line with international standards- (Act 70 interception/ Section 252A CPA)
Maintain and further develop enforcement capabilities

Create “on-line” operational reporting mechanism capacity in order to identify prevailing cybercrime trends/phenomenon, with specific focus on the accumulation of technical data, which, during an analytical process will identify “common denominated” information/evidence and unique patterns of criminal behavior, furthermore, through intervention (once being aware thereof) prevent the continuation of such identified thread.

Establishment “workstation” infrastructure- inclusive of physical infrastructure and software design/maintenance/hosting associated with foreseen ICT infrastructure

Training of identified “on-line” DPCI investigators

Establishment of internal processes/ procedures/ investigative methodologies/best practices in line with international standards
Law enforcement agencies across the globe are continuously focusing on developing investigative/forensic methodologies in addressing cybercrime - be sensible for DPCI to allow research in the field of cybercrime

The variety of digital evidence represents a key component of police investigations and a potential source of evidence that could prove critical in supporting the prosecution of different types of crimes

BROADER THAN COMMERCIAL CRIME PLATFORM

Often the situation that cybercrime has elements of an underlying “traditional” crime. Computers frequently provide a means to aid in the commission of a traditional crime …a computer is used to help implement the offence

Electronic evidence can play a role with regard to almost any offence

Thus be sensible Electronic Crime Unit to extend its supporting role from Commercial to also include Organised Crime/Corruption platform

Proposed-Current human resource capacity to be enhanced
Urgent need - audio/audio visual equipment- setting up of interview rooms (mobile)- interviewing of witnesses/suspects- proper record of proceedings

Identified National Cybercrime Priorities – led to establishment of National Cybercrime Task Team’s (NCTT)

DPCI, at present, not adequately equipped to address cybercrime

Challenge:
Electronic Crime Unit capacity largely at Head Office Level
No similar supporting structures at Provincial Level

Proposed Solution:
Decentralisation of ECU structure
THANK YOU

pietersent@saps.gov.za
ecu@saps.org.za