HAWKS
DIRECTORATE FOR PRIORITY CRIME INVESTIGATIONS

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

Workshop for Policy Design towards Digital Security, Cybercrime and Cybercrime Prevention
Emperors Palace
21 August 2015

CYBERCRIME

A SOUTH AFRICAN PERSPECTIVE

Theme for Digital Wellness Workshop

African Centre of Excellence for Information Ethics (ACEIE)/Civilian Secretariat for Police (CSP)

Serve and Protect in a digital safe and Cybercrime free South Africa

Developing:

- Policies (you need a plan that can work)
- Structures (you need to operational-lize the plan and place human resources / other resources within the structure)
- Skills (training your personnel)
- Guidelines (operational investigative methodologies)

for a professional South African Police Service (National Development Plan)

Scope of presentation

-Establishment of Specialised capacity/Mandate of Directorate/Structures within Directorate (4-8)

-SAPS Strategic Plan/SARPCCO (14-15)

-Cybercrimes and Related Matters Bill (17-19)

-An introduction to computers and some generic computer principals (20-22)

-Legislative-/Technological investigative-framework (23-40)

-Identity theft & fraud/Gaining access to personal information/Intervention strategies (41-46)

-Case Study/Investigative results (47-61)

-Challenges for Law Enforcement (62-63)

Scope of presentation

-Understanding cybercrime phenomenon (64)

-Cybercrime estimate/action plan (65-66)

-South African experience/Lessons learned (69-70)

-A futuristic approach in addressing cybercrime/ Maintain and further develop enforcement capabilities (72-79)

-International cooperation (80-82)

-Operational best practices (83)

-Most Prevalent Crime Threats (84)

-Significant/Noteworthy Successes (85-86)

-Way forward (87)

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 (JUSTICE, CRIME PREVENTION AND SECURITY) 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

The National Cyber-security Policy Framework **sets out the** National Cybercrime **Policy outlining the government's approach to addressing cybercrime**

The effective implementation of the Policy will result in:

Reduction of direct harms of cybercrimes

Increased public confidence in the safety and security of the cyberspace

Public-private partnerships to combat cybercrime

National Cybercrime Policy **based on following approaches**:

Effective law enforcement/criminal justice responses

Need for an approach to countering cybercrime that balances enforcement/prevention, thus includes activities pertaining to combating of cybercrime in relation to:

- prevention
- detection /intelligence-led investigation /establishment of specialized investigative capacities/prosecution

Cross-cutting activities

Policy ensure coordination/ protect national security/national critical information infrastructure

Coordinated approach bring together law enforcement/business/civil society in partnerships- required to address cybercrime/promote interaction with stakeholders

Increased reliance on Information Communication Technology (ICT)

Challenges for traditional law enforcement

Need for interaction with international stakeholders/engage other countries/institutions in terms of bilateral/multilateral measures to address cybercrime

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…"

SARPCCO-General Phiyega-Oct 2014

"Technological developments are trending globally, increasing the ***threat of cybercrime***. At ground level, we are still faced with a ***challenge of responding to cybercrime***. When a complainant reports a crime on hacking or any other related computer crime, we are still left wanting.

We still need to ***develop, train and equip*** our police officers to be able to respond to these types of crimes and complaints. However, these technological developments do not only present challenges, but opportunities for us to embrace technology and step up our game in this regard. When criminals resort to technology, ***we should be a step ahead. We need to have the right expertise***.

We need to stay abreast of trends in the scourge of cybercrime. ***Smarter policing*** of our region and ***pro-activity will lead to the success of our strategies***"

Widespread use of internet has brought with it an increasing number of traditional and new crimes that can now be committed in cyberspace

Threats posed by **cybercrime** are **constantly evolving**

Expected that rapid development/exploitation of computers/electronic communication technologies will continue to accelerate, with a concomitant increase in cybercrime threats and incidents

Cyber criminals becoming more sophisticated/continue to develop malicious software /devise improved methods for infecting computers and networks

Cybercrime varies from relative insignificant transgressions to transnational organised crime

Extent of cybercrime difficult to quantify- generally underreported

Cybercrimes are commonly considered as **falling into one of two categories:** (A) new offences committed using new technologies- (B) existing offences committed using new technology, where networked computers and other devices are used to facilitate the commission of an offence----Cybercrime investigations are technically complex

Cybercrimes and Related Matters Bill

Cybercrime Policy aligned to new draft Cybercrimes and Related Matters Bill- which is currently under construction

Important aspects:

- Creates offences/impose penalties
- Regulate jurisdiction of courts/powers to investigate, search and seize
- Propose establishment of a 24/7 point of contact/National Cybercrime Centre/various structures to deal with cyber security
- Regulates the identification/declaration/protection of National Critical Information Infrastructures
- Provides President may enter into agreements with foreign States/territories to promote cyber security
- Repeal/amend certain provisions of Electronic Communications and Transactions Act, 2002

Cybercrimes and Related Matters Bill

SAPS Responsibility according to the Bill :

Establishing of 24/7 Point of contact and National Cybercrime Centre

Clause 50 of the Bill makes provision for the establishment of a 24/7 Point of Contact

In terms of clause 1 a 24/7 contact point is defined to mean:

> 'a designated point of contact, which is available on a 24/7 basis, in order to ensure assistance in cyber related matters'

Same scope on establishment and responsibility of the 24/7 Point of Contact is also extensively described in the draft Cybercrime Policy

Clause 54 of the Bill makes provision for the establishment of the National Cybercrime Centre which is proposed in the Cybercrime Policy

24/7 Point of Contact /National Cybercrime Centre are two of the seven structures featured in the Bill- the structures will resort under the Cabinet member responsible for Policing/under leadership of the National Commissioner

An introduction to computers and some generic computer principal

- **Data-** information converted into a digital form
- **Digital-** is the use of a binary code to represent information
- **Binary data-** broken down into its smallest unit (capable of being represented/recognised by a computer) called a bit
- **Bit-** represents one of two values, on or off- electronic devices are powered by electricity, which has only two states, on (digit one “1”) or off (digit zero “0”)
- **Byte-** when 8 bits are grouped together as a unit
- **Byte represents information-** provides enough combinations of zeros and ones to represent 256 individual characters
- Combination of one and zeros represent characters are defined by **patterns called a coding system**, which makes it possible for humans to interact with a digital computer that recognize only bits
- **Information-** end product of data processing(8)

An introduction to computers and some generic computer principal

- Computer system (9)
  - Computer hardware (10)
  - Computer software (11)
  - Categories of computer systems (13)
    - Personal computer
    - Handheld computer
    - Internet appliances
    - Servers
    - Mainframe
    - Supercomputer
  - Stand-alone computing environments (14)
  - Network computing environments (15)
    - LAN/WAN/MAN (18)

An introduction to computers and some generic computer principal

Define Cybercrime

Involves computer and/or computer network, *or*

involves any means or device that can create, collect,
collate, process, store, access, transmit, receive, modify or destroy data, or otherwise render data ineffective (where data means an electronic representation of information in any form), *or*

which is complex in nature and requires specialised
technology related investigation skills

Legislative framework

United Nations Convention against Transnational Organised Crime

Article 2(b) of Convention

"serious offence" means "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty"

South Africa- a signatory to Convention- ratified Convention/subsequent Protocols-- SA party to convention which represents an International effort to combat organised crime

Council of Europe's Cybercrime Convention (Budapest)

proved a sound basis for essential cross border law enforcement cooperation required to combat cybercrime

Serve as a purpose built mechanism on which countries can fashion own domestic legislation and enhance international cooperation in relation to cybercrime

SA signed Convention on cybercrime- not ratified it

Legislative framework

Council of Europe's Convention on Cybercrime proved a sound basis for essential cross border law enforcement cooperation required to combat cybercrime

Serve as a purpose built mechanism on which countries can fashion own domestic legislation and enhance international cooperation in relation to cybercrime

SA signed Convention on Cybercrime- not ratified

Legislative framework

African Union Convention on Cyber Security/Data Protection (adopted/focus on)

- Addressing legislative measures as deem effective
- Substantive/procedural provisions reflect international best practices
- Cardinal principle of cooperation in application of law against cross-border crime reposes on the fact that the laws under which such cooperation is sought should be uniform in terms of prohibited conduct and application procedure
- Adopting such measures as it deems necessary to foster exchange of information and sharing of quick/ expeditious/reciprocal data
- Ensuring legislative measures adopted in respect of material/procedural provisions reflect international best practices/integrate minimum standards

Legislative framework

African Union Convention on Cyber Security/Data Protection

- Ratified the Convention

- Prioritise implementation of cybercrime aspects by:

  Enacting comprehensive/harmonise cybercrime laws

  Embracing capacity building efforts by offering training to identified stakeholders responsible for addressing cybercrime

  Establishing appropriate institutions to address cybercrime

  Enhancing formal/informal international cooperation and develop capacity to investigate “online” crimes

Legislative framework

Other legal instruments

- East African Community (EAC) Legal Framework for Cyberlaws
- Economic Community of West African States (ECOWAS) Directive on fighting Cybercrime
- Common Market for Eastern and Southern Africa (COMESA) Cyber Security Model Bill
- Southern African Development Community (SADC) Law on Computer Crime and Cybercrime
- United Nations Convention Against Transnational Organised Crime- United Nations General Assembly Discussion Guide (A/CONF.222/PM.1 dated 19 July 2013) focusing extensively on the combating of transnational organised crime, specifically in relation to the phenomenon cybercrime

Legislative framework

Electronic Communications and Transactions (ECT) Act (25/2002) objectives:

- To provide for facilitation/regulation of electronic communications/transactions
- To provide for development of a national e-strategy
- To promote universal access to electronic communications/transactions
- To prevent abuse of information systems
- To encourage use of e-government services

Legislative framework

Electronic Communications and Transactions (ECT) Act (25/2002) objectives:

To provide for facilitation/regulation of electronic communications/transactions

To provide for development of a national e-strategy

To promote universal access to electronic communications/transactions

To prevent abuse of information systems

To encourage use of e-government services

Legislative framework

Sec 86- criminalizes unauthorized access to, interception of or interference of data

- intentionally accesses/intercepts data without authority/permission-guilty of an offence-person convicted liable to a fine OR imprisonment for a period not exceeding 12 months
- intentionally/without authority interferes with data, which causes such data to be modified/destroyed or otherwise rendered ineffective-guilty of an offence-person convicted liable to a fine OR imprisonment for a period not exceeding 12 months

Legislative framework (86)

- unlawfully produces/sells/offers to sell/procures for use/designs/adapts for use/distributes or possesses ANY DEVICE, including computer program which is DESIGNED PRIMARILY TO OVERCOME SECURITY MEASURES for protection of data, or performs any of those acts with regard to a password/access code or similar kind of data with intent to unlawfully utilize such item-guilty of an offence-person convicted liable to a fine OR imprisonment for a period not exceeding 12 months

(protect computer networks against hacking/illegal access)

Legislative framework (86)

A person who utilizes any device or computer program (as mentioned *supra*) in order to unlawfully overcome security measures designed to protect such data or access thereto, guilty of an offence-guilty-person convicted liable to a fine OR imprisonment for a period not exceeding 5 years

A person who commits any act described Sec 86 with intent to interfere with access to an information system so as to constitute a denial of service to legitimate users, guilty of an offence-person convicted liable to a fine OR imprisonment for a period not exceeding 5 years

Legislative framework

Sec 87- provides statutory versions of the common law crimes of extortion/fraud/forgery specifically tailored to the electronic medium-person who performs/threatens to perform any of the acts described in Sec 86, for purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such actions, or by undertaking to restore any damage caused as a result of those actions**/**person who performs any of the acts described in Sec 86, for purpose of obtaining any unlawful advantage by causing fake data to be produced, intent considered/acted upon authentic, guilty of an offence-person convicted liable to a fine OR imprisonment for a period not exceeding 5 years

Legislative framework

Sec 88- criminalizes any attempt, aiding and abetting of offences referred to in Sec 86/87:

-directed at so-called accessories after the fact, person(s) that did not commit the offence itself, but assisted the perpetrators afterwards

(concealing perpetrator from law enforcement)

Legislative framework

Sec 90- provides for jurisdiction of courts:

-offence committed in RSA

-any act of preparation towards the offence or any part of the offence was committed in RSA, or any result of the offence has had an effect in RSA

-offence committed by SA citizen or person with permanent residence or person carrying on business in RSA

-offence committed ship/aircraft registered in RSA or on voyage/flight to/from RSA at time offence was committed

Legislative framework

Is computer printout a data message?

- Narlis v S A Bank of Athens 1976
  - computer printout cannot be received as evidence ito S 34 Civil PA
- Mashiyi 2002
  - information contained in disputed document-after treatment by arrangement, sorting, synthesis and calculation by the computer
- Ndlovu v Minister Correctional Services 2006
  - printout copy and not original, printout was a computer printout and should not be admitted in evidence unless properly proved

Legislative framework

- S 222 CPA
  - of no assistance to the prosecution in regard to admissibility of computer printouts
- S 221 CPA
  - possible vehicle to allow admission on dispute printouts?
  - Ruled computer printouts to be inadmissible

Electronic Communications and Transactions Act 25/2002-S 15

- Aim to place electronic information on same footing as traditional paper-based transactions
  - Data message
    - “data generated, sent, received or stored by electronic means and includes-voice, where the voice is used in an automated transaction, and a stored record”
  - Data
    - ”electronic representations of information in any form”

Legislative framework

Is computer printout a data message?

PRINTOUT IS CLEARLY A DATA MESSAGE

Technological investigative framework

Challenges (legal/technical/resource)

Evidence is overwritten

On-line criminals become more sophisticated

Anonymous (anonymity) nature of Internet-investigate/prosecute criminals international arena

Users connect to Internet from anywhere in the world-telecommunication systems has its own protocols and routing of traffic

Legal challenges

Obtaining information/evidence from foreign countries required legal tools necessary to investigate cybercrime lag behind technological/structural/social changes

Ubiquity/connectivity of every workstation to global community have ramifications-to be worked out by legislators/legal system (43)

Technological investigative framework

Resource challenges

Resources required in cyber/computer related investigation substantial

While the crime may be HIGH TECH, investigating it involves a substantial amount of TRADITIONAL investigative work as well as HIGHLY TECHNICAL work (log information/technical analysis)

Computer/Cyber-forensics defined

Involves preservation/identification/extraction/documentation/interpretation of computer media FOR evidentiary/root cause analysis

Process of extracting data from computer storage media/guaranteeing its accuracy/reliability

Basic methodology **ACQUIRE**(without altering/damaging the original)/**AUTHENTICATE**(recovered evidence same as original seized data)/**ANALYSE**(the data without modifying it)

(45)

Identity theft/fraud

One of the leading contributors to a successful fraud SA Banking Association

Costs the economy around R1 billion a year Compuscan Registered credit bureau

Identity theft is rife for various reasons and is the white collar crime of choice because it is easily done Bowman Gilfillan Inc

South Africans relaxed lifestyle make them easy targets for identity theft-SAPS not adequately equipped to handle this type of crime, but made easier because South Africans do not destroy their documents properly

Hillcrest Private Investigator Rick Crouch

Identity theft/fraud

Unauthorized acquiring /utilization of another persons (victim) personal identifying and/or financial information for the sole purpose of assuming that persons identity in order to make unlawful transactions/purchases

- Imposter obtain key pieces of personal information
- Victim endure adverse consequences if held liable for perpetrators actions cost you time/money destroy your good name
- Determining the data breach/identity theft is challenging, primarily because identity victims do not know how their personal information was obtained
- Global threat- serious impact on economy
- Identity theft not a industry specific crime
- Influx of technology caused identity theft/fraud to grow at an alarming pace

Boiler rooms- “illegal high-pressure sale operations pushing overpriced and even non-existent shares”

Fraudulent document manufacturing plant/outlet
Public Internet facilities

DHA Smart ID Card

DHA/Sabric partnership

- online fingerprint/biometric verification system
- DHA allow banking platform to verify the identity of prospective/current clients
- important measure in assisting banking platform preventing identity theft related crimes

S A FRAUD PREVENTION SERVICE (SAFPS)

target area-men 30 to 40 age group most at risk

2009 TO 2011-5940

KPMG

typical fraudster-men 36 to 45 age group

2011 Global Analysis of Fraud Trends

ALL INDIVIDUALS ARE AT RISK REGARDLESS OF AGE OR GENDER

2012 SAFPS Chairman's report

number of fraud filing increased by 27%

CIFAS International highly acclaimed fraud prevention UK company

"…identity theft cases represent 48% of all their fraud records and account take over fraud has rocketed by 300% in just 5 years"

Gaining access to personal information

Dumpster diving

rummaging through trash looking for bills/documents

Skimming

credit/debit card particulars unlawfully obtained through the use of storage device while card is being processed for payment

Phishing

Criminals pretend legitimate financial institution-forward spam/pop-up messages requesting personal information trojan spy software

Changing of address

Divert billing information correspondence to different location by changing the delivery address

Mail theft

Bank/card statements stolen from mail

Intervention strategies

Deter

deter identity thieves by safeguarding your information

Detect

detect suspicious activity by routinely monitoring your financial documents

Defend

Defend against identity theft the moment you become suspicious

Strategic intervention strategy based on a two-fold approach

Firstly:

Consumers need to become more vigilant in their financial dealings and the protection of their personal information

Secondly:

Businesses need to implement appropriate systems to detect/ prevent/having standard operating procedures (SOP's) in place to adequately address identified fraud phenomenon

ENTER THE ELECTRONIC CRIME UNIT

HAWKS
DIRECTORATE FOR PRIORITY CRIME INVESTIGATIONS

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 R e s e r ve 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 ABC Bank

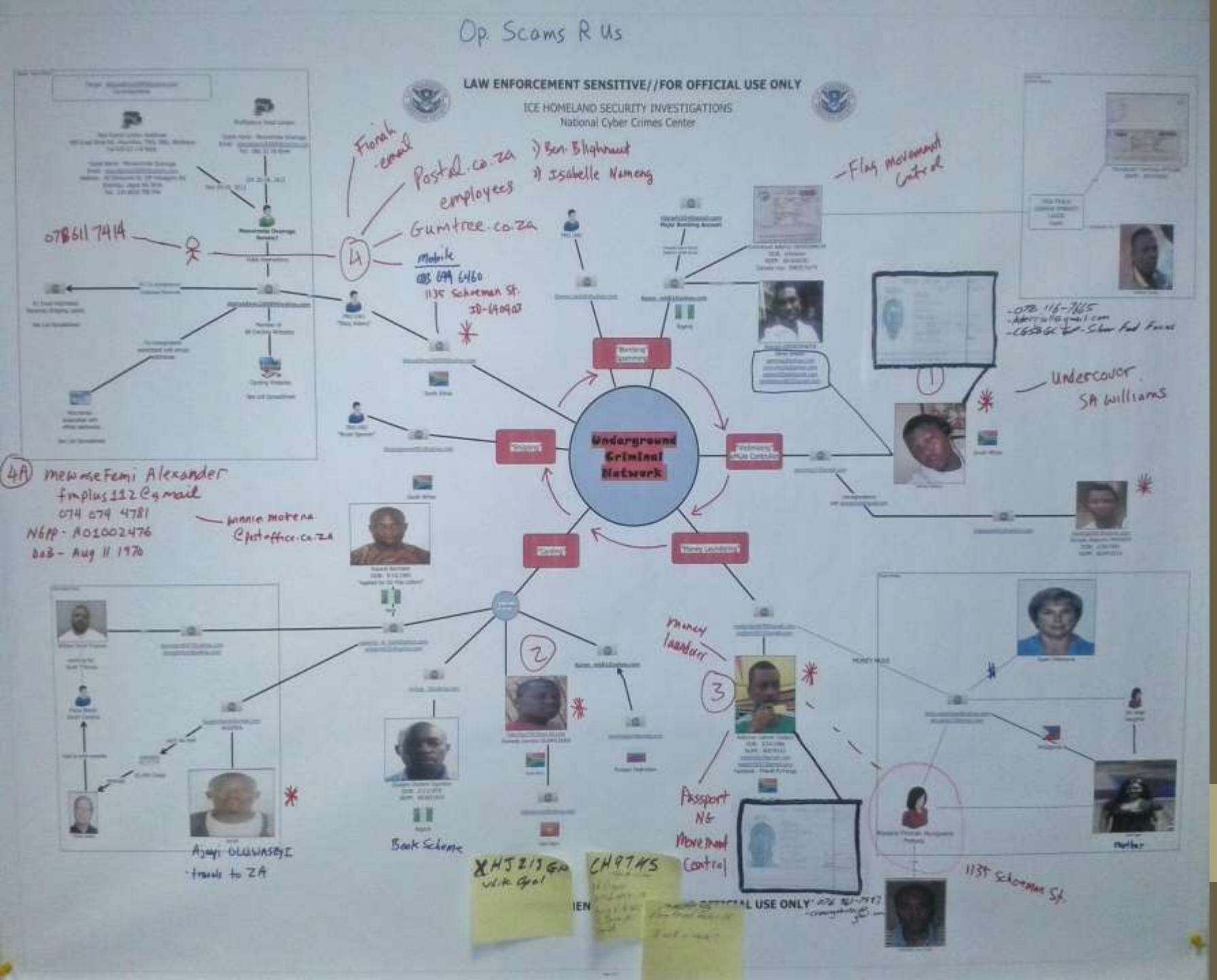
February 2012 –Mr Bxxx Mxxx Txxx arrested-On 22 February 2012 sentenced 25 years imprisonment

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 sentenced15 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


Op. Scams R Us
LAW ENFORCEMENT SENSITIVE//FOR OFFICIAL USE ONLY
ICE HOMELAND SECURITY INVESTIGATIONS
National Cyber Crimes Center
Underground Criminal Network
Banking/Spamming
Phishing/Web Defacing
Money Laundering
Carding
Hacking
Fiona email
Postal.co.za employees
Gumtree.co.za
Mobile
1) Ben Blightwood
2) Isabelle Nameng
Flag movement Control
078 611 7414
4
4A
mewase Femi Alexander
fmplus112@gmail
074 079 4781
N6P - A01002476
DoB - Aug 11 1970
winnie motena @post-office.co.za
1135 Schoeman St.
ID-690907
Undercover SA Williams
078 116-7165
1
2
3
Money launderer
Passport N6 Movement Control
Bank Scheme
Ajayi OLUWASEYI
travels to ZA
XHJ213GP
CH97MS
1135 Schoeman St.
Mother

Identified enterprise linked to known **East-European/Vietnamese cyber crime rings** perpetuating criminal underground economy relating to internet

Nexus between identified International crime rings and SA based West African criminal enterprise, supported by SA Nationals, evolved around unlawful **obtaining confidential credit card/personal particulars** of International Banking/Financial Institutions

Enable, via the **internet platform**, to purchase electronic equipment

On receipt of illegally obtained merchandise, the syndicate operation provided for an elaborate/sophisticated **distribution network**

Phenomenon supported- sophisticated operation relating to **spamming** e-mails (job- and dating websites)

INVESTIGATIVE RESULT scams-r-us

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

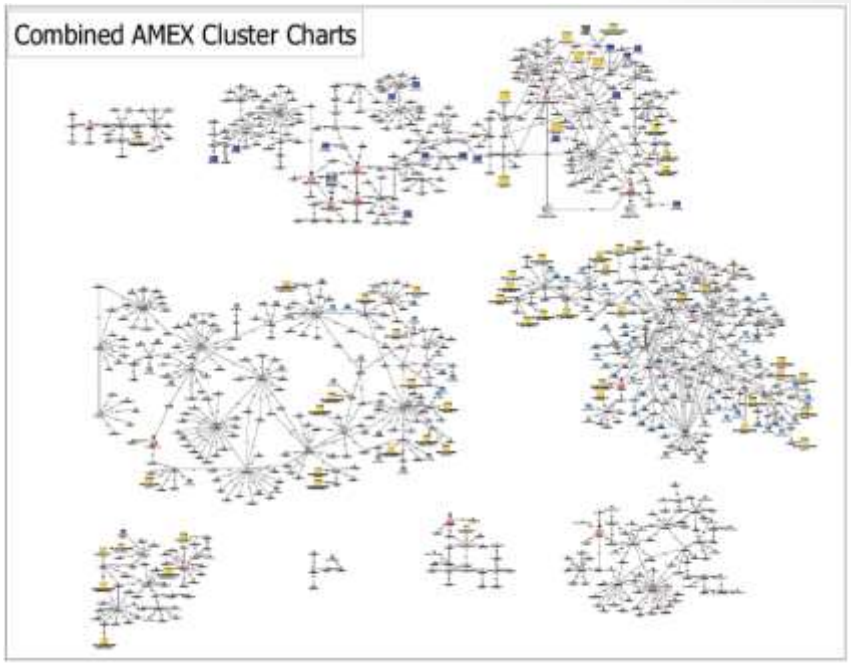
First Leg of Scams-R-Us May 2014- Simultaneous take-down operation in SA/US/Canada (INTERPOL)- search seizure/arrests/forfeiture accused in SA extraditions authorized

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

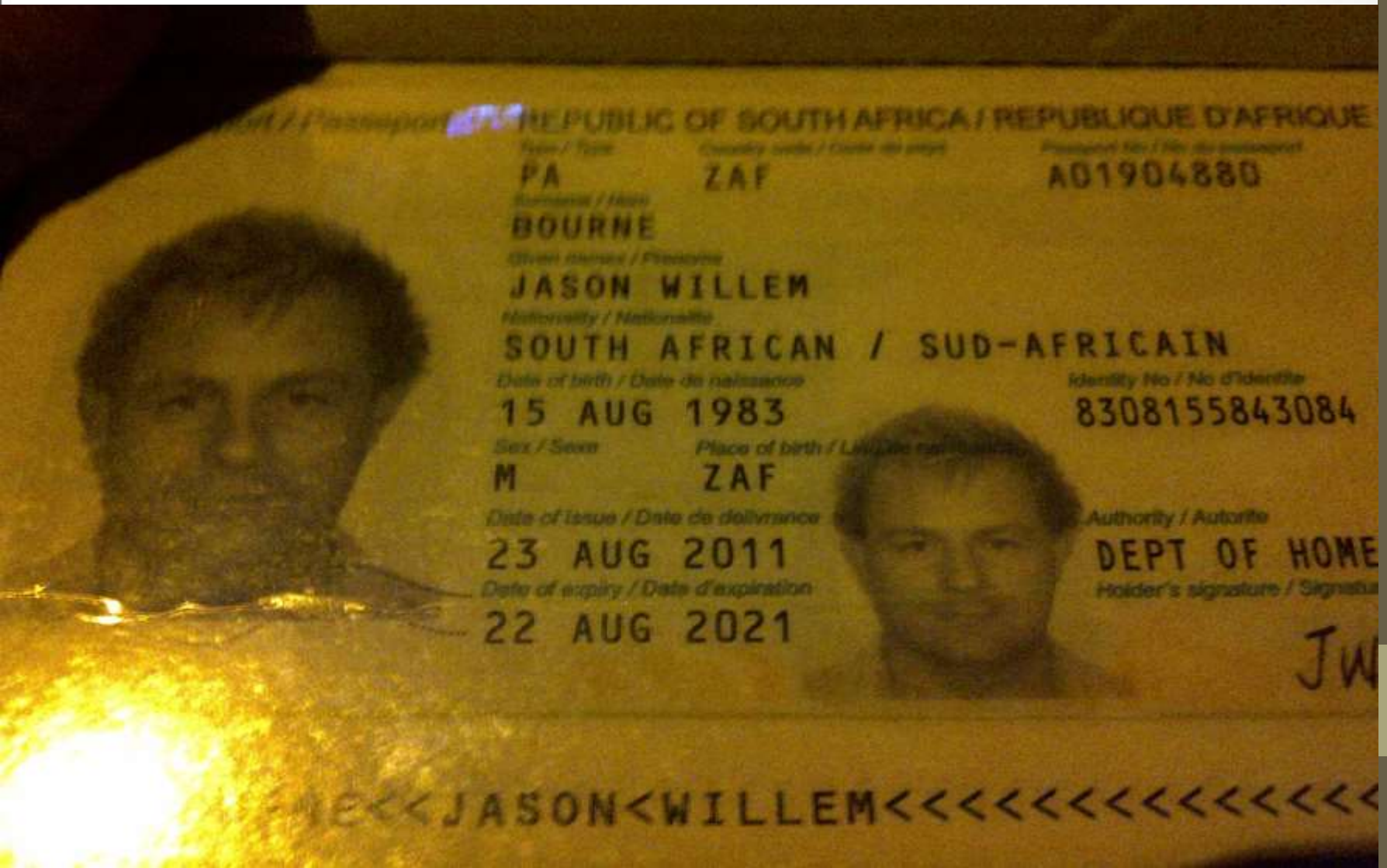

Combined AMEX Cluster Charts

MAJOR INVESTIGATION NATIONAL PROJECT/PROGRAM	PHENOMENON/THREAT
ABC bank	Cyber Crime Intrusion (CCI)
Scams-R-Us	Transnational Hacking/Mass Marketing Fraud
F*** F**	Credit/Debit Card and Card not present Fraud
Eskom	Cyber Crime Intrusion (CCI)
V***/ N*****	Cyber Crime Intrusion (CCI)
S*******	High Tech Skimming Fraud
I*******	High Tech Skimming Fraud
G********	Handheld Skimming Fraud
I****** E****** C********* (***)	Cyber Crime Intrusion (CCI)
Gautrain Management Agency	Cyber Crime Intrusion (CCI)
G*******	Sim Swap/Phishing
RTMC- Road Traffic Management Corporation	Cyber Crime Intrusion (CCI)
Mini Cooper	Identity Theft /Fraud, Sim Swop/Phishing
No.11	Identity Theft /Fraud, Sim Swop/Phishing
M*****	Asset Base Fraud-Home Loan Application
A********	Asset Based Fraud- Home Loan Application
R*********	Asset Based Fraud- Vehicle Application
W**********	Asset Based Fraud- Home Loan Application
D**	Cyber Crime Intrusion (CCI)

CAPUT LUPINUM

WOLF's HEAD

WE EVEN HAVE OUR OWN JASON BOURNE AKA MATT DAMON



Challenges for Law Enforcement

Traditional investigative methodology approach in addressing cybercrime threat, **does not effectively address the business systems in relation to cyber crime**

Upsurge in cybercrime within the financial environment **poses a threat** to our democracy/economy

Imperative that strategies be developed in order to successfully eradicate cybercrime

Greater use of encryption/access protection poses a growing challenge of extracting evidence from computers

Reluctance of victims to report offences-many victims are unaware that their computers had been compromised (underreporting)

Strategies/measures against cyber crime would have to follow a criminal justice rationale, linked to broader crime prevention and criminal justice policies, aimed at contributing to the rule of law/the promotion of human rights (Adv Paul Louw- stick to the scrip)

Understanding cybercrime phenomenon

What is the extent and impact of the cybercrime phenomenon manifestation, with specific reference to the impact on financial (banking) related cyber crime fraud?

What is the extent to which Law enforcement can effectively address the identified cybercrime phenomenon?

How can the cyber crime priority threat- and risk assessment process be identified and defined, in order to establish the criminal business enterprise?

What strategies, action plans and operational initiatives should be developed, together with identified stakeholders, to effectively address the identified criminal business enterprise, from a combating/preventative/investigative/prosecutorial perspective?

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

South African experience

Commercial crime increasingly show unique **transnational organised crime** characteristics

Cybercrime/electronic related crime equally present similar international and organised trends

Cybercrime clearly reflect elements of transnational organised crime and has evolved in a **sophisticated** crime phenomenon, with specific reference to cyber related fraud scams

Lessons learned

Strategic outcome in successfully eradicating cybercrime 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

Lessons learned

Cybercrime is generally **transnational** and **organised** in nature

Difficult/time-consuming to **secure evidence**

Despite expensive **security measures**, criminals will counter it successfully

Corruption of corporate and state employees

Sophisticated techniques employed by criminals

Attempts at investigation involving computers often fail because of **mistakes made at a very early stage**- essential digital evidence is ignored/destroyed/compromised/inappropriately handled

Lessons learned

Difficult, time-consuming to **understand crime threat (Faceless problem)**

The approach of **“follow the money”** not always guarantee success and it is time consuming

Cyber crooks often **use known criminals** to receive the proceeds of crime

Difficult to **id**entify and successfully **prosecute** cyber criminals International cooperation MLA/Communication with International role player on informal basis

Hand-in-glove approach with prosecution most effective method

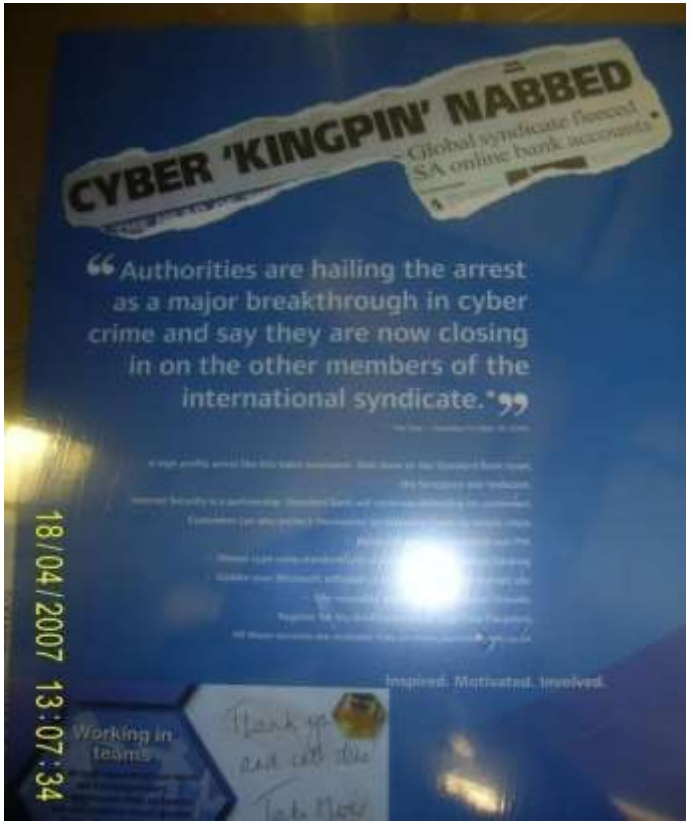

25/05/2006 09:35:22


2006/10/05 18:23:46


2006/10/06 15:45:25


10/05 11:41:53

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)

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 denominating" 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

External Expert Working Group

(Subject matter experts within the private sector) providing assistance/guidance to law enforcement management in terms of continuous Strategic development/Operational best practices

EMBRACE A COMMON AND SHARED RESPONSIBILITY IN COUNTERING CYBERCRIME

Cyber Threat Intelligence Intervention Centre (CTIIC) FOR AFRICA ?

Cyber Academy ?

(Institution of higher education and law enforcement working together)

Generic First Responder Training (Introduction to electronic Crime Scene) to all law enforcement officials- training model developed/registered and pilot project successfully implemented

Commercial Crime Level 3 –Investigation of Cyber Crime

Specialized Digital Forensic Training

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


COPPED by SA's CYBERCOPS

International cooperation

Council of Europe's Convention on Cybercrime **proved a sound basis for essential cross border law enforcement cooperation** required to combat cybercrime

Serve as a purpose built mechanism on which countries can fashion own domestic legislation and enhance international cooperation in relation to cybercrime

SA signed Convention on Cybercrime- not ratified

SA has laws dealing with cybercrime, not in one framework, Electronic Communications & Transactions (**ECT**) Act- **fail to recognize seriousness** of cyber offences

International cooperation

Council of Europe's Cyber Crime Convention enhances:

Mutual Legal Assistance (MLA)

comprehensive powers to expedite preservation of stored computer data and partial disclosure of traffic data

make production orders

search computer systems

seize stored computer data

enable real-time collection of traffic data

intercept the content of questionable electronic data

International cooperation

Establishment of US/SA Cyber Working Group:

Identified areas of mutual interest

Strengthening opportunities for cooperation

Focus on technical assistance/capacity building/training/sharing of best practices

Foreseen future meetings will include private sector/civil society stakeholders

Operational best practice

Project driven/major investigations

Stakeholder partnership

Investigative strategy

Prosecutorial strategy

Focus on Asset Forfeiture/Revenue

Value chain analyses

Strategic Intervention Strategy

Focus on IMPACT with regard to crime threat/phenomenon

Most Prevalent Crime Threats

Crypto-locker

data intrusion, data encryption and extortion with virtual (bitcoin) currency in order to be forwarded the software “key” to de-crypt the compromised data

Jackpotting

ATM intrusion

Transnational Mass Marketing Fraud

West African Criminal Enterprise**S** operating from within South Africa-fraud against e commerce merchants utilizing PII and financial data and anonymous-asation of their true connection via virtual private network (VPN) and underground SOCKS proxy services- over 200 new syndicate members identified in a number of different countries as part of the broader criminal business enterprise

Dormant accounts

Significant/Noteworthy Successes

Park Road CAS 682/06/2014

Section 252A Operation-Postbank R30M- arrest of Mr Mxxx Mxxx- succesfully prosecuted

Program Scams R Us

First Leg: Following simultaneous international takedown operation (May2014)-arrested targets found to be extraditable-process started-urgent application in High Court to prevent extradition process- Judgment-Mutual Legal Assistance (MLA)-obtaining of Section 7/8 affidavits ongoing

Second Leg: December 2014- Arrest Heathrow Airport by UK Law enforcement-preservation order on properties- hearing scheduled 9 April 2015 North Gauteng High Court- 25 May 2015 forfeiture order granted-AFU will keep us informed re selling of the assets and repatriation of funds

Eskom (Project VXXXX)
Olifantsfontein CAS 427/11/2014- 21 November 2014- intelligence led operation- Solomon Pxxxx/Kgomotso Mxxx/Neo Mxxx arrested- exposure R3,5 B

XXC intrusion- Enquiry ECU 26/18/2 (756)
December 2014 Search and Seizure Operation, Cape Town- ongoing investigation-possible suspect identified

Gautrain
23 October 2014-intelligence led operation- Obakeng Israel Bxxx arrested-exposure R800M

Mini Cooper (Project NoXXX)
33 CAS dockets centralized-31 accused before court-identity theft and boiler rooms- Project 11 second phase- targets have been identified

Zim drill bits- Enquiry ECU 26/18/2 (312)
Arrest operation Cape Town

Way forward

Identify vulnerabilities in relation to:

SA criminal justice system/rule of law/unique SA cyber security landscape identified as contributing inhibiting factors in successfully addressing cyber crime threat

Successful criminal prosecution by law enforcement agencies/prosecuting authorities depend essentially on the availability of *prima facie* admissible evidence

Develop a strategy to successfully eradicate cyber crime will contribute to Government's Delivery Agreement in that **"ALL PEOPLE IN SOUTH AFRICA ARE AND FEEL SAFE"**

Imperative strategy meet international benchmarked standards be inclusive of a multi stakeholder approach in its:

Design

Implementation

Management

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