HAWKS
DIRECTORATE FOR PRIORITY CRIME INVESTIGATION

Cybercrime in South Africa

FinTech Exploitation, Law Enforcement Challenges and Strategic Responses

Misuse of Technology in Financial Crimes (Specialty) Pilot Programme,
31 March - 4 April 2025, Ostia, Italy

03 April 2025

Disclaimer

The information, graphics, and case examples presented in this presentation are intended for educational and strategic discussion purposes only. While every effort has been made to ensure accuracy, some content may be anonymised cases. All images, including process diagrams, are original ideas used with commercial licenses. This presentation was formally approved by the National Head of the Directorate for Priority Crime Investigation (DPCI) for awareness and stakeholder engagement purposes. It does not constitute an official legal opinion or policy document unless otherwise specified.

ABOUT US

Directorate for Priority Crime Investigation

01. Prevent, combat, and investigate National Priority Offences that require specialised expertise and intelligence-driven investigations

02. Enforce laws under Chapter 2 and Chapter 34 of the Prevention and Combating of Corrupt Activities Act, 2004 (Act No 12 of 2004), particularly those involving financial fraud, corruption, and large-scale cyber-enabled crimes.

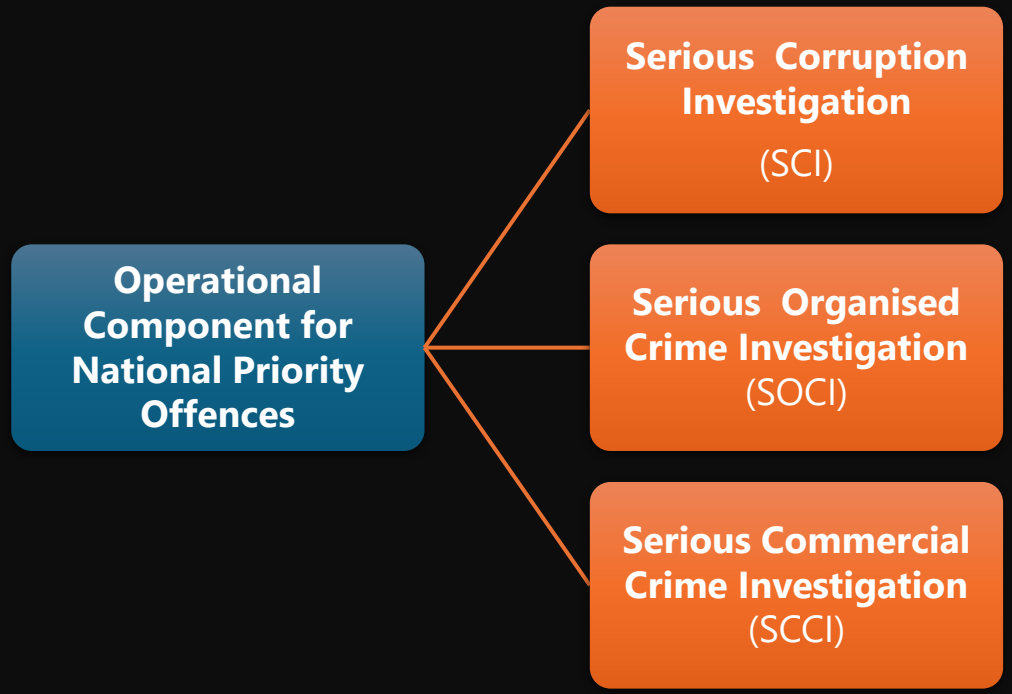


Figure 1: Overview of the Operation Component National Priority Offences

Figure 2: Overview of a Supportive Component for National Priority Offences

Cybercrime Process Flow

The cybercrime response process begins with acknowledging the incoming cybersecurity request, followed by a thorough risk assessment to determine the severity and scope of the threat. A tailored cyber investigative strategy is then developed and implemented alongside essential cyber hygiene practices. This leads into the cyber forensic process, where evidence is gathered and analyzed. Stakeholder engagement ensures coordination across agencies and sectors. Finally, insights gained are used to continuously improve South Africa's cybersecurity posture, enhancing national resilience against future threats.

Case Discussion

Case Discussion

01. Education department investigates illegal sale of matric marks

02. The Fake Loan Application Scam

03. Digital Cybercrime Network

Illegal Sale of Matric Marks

The Edumarks case emerged when students and concerned parties reported a suspicious service offering a fee for early access to matric results. The company, which has been operating since 2021, promised students their National Senior Certificate (NSC) results before the official release date in exchange for a fee.

Commercial Exploitation of Fraudulent Information

- Fraud
- Digital Payment Channels
- Government Protocols
- Fintech platforms

The Fake Loan Application Scam

The fraudulent operation was orchestrated by an organised cybercrime group that developed and distributed a deceptive mobile application. This app falsely advertised easy loans in West Africa through social media.

01/

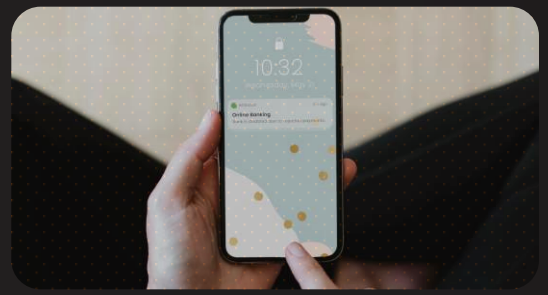
Investigation

The scam involved a malicious mobile app that demanded excessive permissions from users, enabling access to personal data. Victims faced harassment and blackmail through aggressive debt collection methods. A call centre network was used to pressure repayments. Investigations traced the operation to C2 servers, with South Africa identified as a key hub in the scam's infrastructure.

02/

Crime

- Financial Fraud and Predatory Lending Practices
- Data Privacy Violations
- Cyber Harassment and Blackmail
- Social Engineering and Malware



03/

Fintech

- Digital Loan Disbursement and Collection
- Call Centre and Payment Tracking
- Anonymous Payment Channels

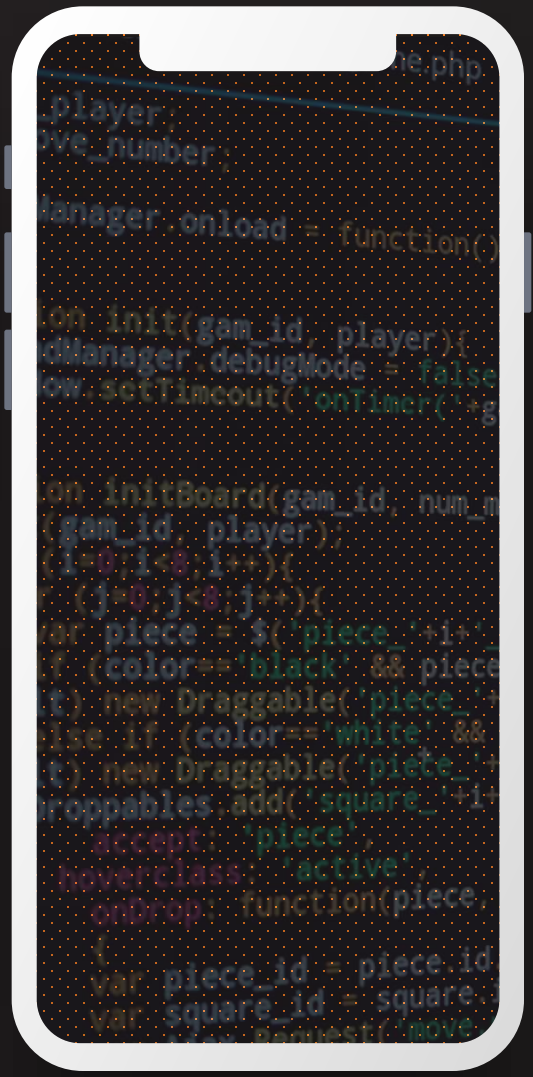
Digital Cybercrime Network

01/

South African Police Service (SAPS) was alerted to suspicious cyber activity on an online black-market forum, which had identified South African users involved in illegal transactions.

Involvement of Financial Technology **/03**

Exploited online anonymity, cryptocurrency transactions, and fintech payment platforms to enable the illegal sale and purchase of stolen data without detection.



02 **Crime Committed**

- Access credentials
- Database dumps
- Personal identification information

Cybercrime →

Challenges in Cybercrime Investigations

Cybercrime investigations are hindered by rapidly evolving technology, cross-border jurisdictional issues, and limited forensic capabilities. The use of encryption and anonymity tools makes tracking perpetrators difficult, while delayed reporting and poor information sharing slow down response efforts. These challenges highlight the need for stronger collaboration, advanced tools, and skilled personnel.

1/ Legal frameworks

2/ Specialised Cyber expertise

3/ Retention of specialised Cyber expertise

4/ Resource Constraints (Human, Financial and Physical)

Strengthening Cybercrime Investigations

Leveraging Open-source Tools

Enhance cooperation with international and local stakeholders

Training and Development

Utilising AI in investigations

The Future of Cybersecurity in South Africa

Cybersecurity Bill 80%

Designated Point of Contact for Cybercrime Act 50%

Development and deployment of Software for Section 54 Obligations of electronic communications service providers and financial institutions 75%

Securing the Digital Future

HAWKS
DIRECTORATE FOR PRIORITY CRIME INVESTIGATION

Compiled by: Kaylan Moodley
Designation: Captain | Commercial Technology Crimes
Email: Moodleyk5@saps.gov.za
Cell: +27 82 565 4847

saps.gov.za/dpci

03 April 2025

Questions and Answers

Let's Secure the Future Together