*IST-Africa 2016 Conference Proceedings*
*Paul Cunningham and Miriam Cunningham (Eds)*
*IIMC International Information Management Corporation, 2016*
*ISBN: 978-1-905824-55-7*

# Classification of Cyber Attacks in South Africa

Renier VAN HEERDEN[1,2], Suné VON SOMS[3], Roderick MOOI[1]
[1]*Council for Scientific and Industrial Research, P.O. Box 395, Pretoria, 0001, South Africa,*
*Tel: +27 12 841 3434, Fax: +27 12 841 4223, E-mail: rvheerden@csir.co.za, rmooi@csir.co.za*
[2]*Rhodes University, Private Bag X1042, Grahamstown, 6140, South Africa*
[3]*University of Johannesburg, PO Box 524, Auckland Park, 2006, South Africa,*
*Tel: +27 11 559 2462, E-mail: svonsolms@uj.ac.za*

**Abstract:** This paper introduces a classification scheme for the visual classification of cyber attacks. Through the use of the scheme, the impact of various cyber attacks throughout the history of South Africa are investigated and classified. The goal of this paper is to introduce a classification scheme that arranges attacks into different classes and sub-classes, which is presented visually. To enhance the visual description, each class has a maximum of three sub-classes, which can overlap. This classification scheme helps to show the diverse impacts of cyber attacks in South Africa. This method of classification can be used for the assessment of any cyber attack and to find similarities between attacks.

**Keywords:** cyber attacks, classification, South Africa.

## 1. Introduction and Overview

The integration of information technology (IT) in our daily lives has created an environment where individuals, businesses and governments are highly dependent on reliable and secure operation of these systems. This dependence on computer systems and networks has created an environment where compromise, loss or damage of these IT systems can lead to massive financial, environmental, social, political or personal damage.

For this paper, any offensive manoeuvre performed against an IT system by an internal or external party is considered to be a cyber attack. As the rapid growth of technology exceeds the development of proper legislation relating to cyber crime, security systems and awareness, individuals, businesses and governments are vulnerable to cyber attacks. Cyber attackers perform malicious acts which target computer information systems, network infrastructure, computer networks or personal devices in order to infect, damage or control the system. Thereafter, the attacker can steal, alter or destroy information accessible via the compromised system. These attacks can have a massive impact (varying from a slow network connection to destroying critical infrastructure).

This paper provides an overview of the diverse impacts of cyber attacks in South Africa through the use of a new classification model. This model enables the user to make comparisons and find trends in a visual manner. The usefulness of the model is illustrated by using it to analyse twelve South African cyber attacks.

In the next section, the classification scheme is introduced. Thereafter, a timeline is provided where twelve of South Africa's largest cyber attacks are discussed. In section 4, the attack examples are categorised according to the provided cyber attack classifications. We then conclude with a discussion (presenting two use cases) and summary of the paper.

## 2. Classification of Cyber Attacks

Cyber attacks can be classified from the point of view of the aggressor/hacker/attack or from the view of the victim/target. Traditionally, cyber attacks are only classified by either the mechanisms or domain of the attack. The Common Attack Pattern Enumeration and Classification (CAPEC) is a comprehensive dictionary and classification taxonomy that has nearly 3000 attack domains and over 4000 attack mechanisms [1]. CAPEC and similar taxonomies have a weakness in that cyber attacks can only be categorised within a single class. The methodology, medium and other factors also influence how a cyber attack can be classified.

In the next section, a timeline of South African cyber attacks is presented. A taxonomy for computer network attacks was developed by [2] which we use to classify the cyber attacks listed in the timeline. The following classes are derived to define cyber attacks [3]: Attacker, Goal, Mechanism, Effect, Motivation, Target, Vulnerability and Scenario.

All of the classes have three main sub-classes by which cyber attacks can be defined. The number of subdivisions was chosen to simplify the classification process, and in the case of the *Target* class one of the sub-classes was subdivided into another three divisions. These classes form the basis from which the cyber attacks are classified and visually represented.

### *2.1 Attacker*

The *Attacker* (also known as Hacker, Cracker, Fraudster, Conman or Aggressor) describes the entity that is performing the attack. The Attacker class consists of the following sub-classes: Hacker, Insider, or Criminal. The *Hacker* sub-class is an combination of Hacker, Cracker and Script kiddie [4], referring to a skilled computer user who is willing to break (hack) security. The *Insider* sub-class refers to a person who is in some trusted relationship with the target [5]. *Criminal* refers to an attacker that by definition is malevolent.

### *2.2 Goal*

The *Goal* refers to the purpose of the attack, which can be divided into the following sub-classes – *Stealing*, *Disrupting* or *Changing Data* – corresponding to the traditional Confidentiality, Integrity and Availability (CIA) information security principles and outcome classes [6].

### *2.3 Mechanism*

The *Mechanism* represents the attack methodology. The Common Attack Pattern Enumeration and Classification (CAPEC) group developed an exhaustive attack mechanism taxonomy[1]. The subclasses include: Denial of Service, System Abuse and Information Gathering. The *Information Gathering* sub-class refers to the mechanisms used to acquire information about a possible target. Popular information gathering mechanisms include scanning and social engineering [7]. The *System Abuse* sub-class refers to the abuse of computer resources, such as bandwidth, computer memory or storage space [8]. *Denial of Service* refers to attacks that use accepted communication protocols in malicious methods or in overwhelming numbers to deny user access [9].

[1] http://capec.mitre.org/data/index.html

### *2.4 Effect*

The *Effect* of the cyber attack can be described as: Minor, Major or Critical. These high level classifications were chosen since it is difficult to quantify the exact extent for many of the cyber attacks listed in the timeline. *Minor* damage can be defined as recoverable damage and *Major* as non-recoverable damage. *Critical* refers to damage where the target ceases to operate (such as bankruptcy) [10].

### *2.5 Motivation*

The *Motivation* for a cyber attack can be one of the following [3, 10]: Political, Criminal/Financial or Fun/Personal. These motivations are not exclusive, thus a cyber attack can have multiple motivations. *Fun/Personal* refers to hackers looking for a challenging problem. Solving the problem is the motivation, not the effect of the attack. For example, some worms and viruses were not developed with any harm intended, but got out of control beyond the creators' intention [12]. *Political* motivation refers to motivation that has a political aspect. This political aspect can be national interest by spies, political reasoning or vigilantes type groups [4]. *Criminal/Financial* refers to hacking for financial gain or other criminal intent.

### *2.6 Target*

The *Target* refers to the physical devices that are targeted by a cyber attack. These include: Computer Systems, Mobile Devices or Network Infrastructure. The final target may be a human, but all attacks are aimed at a specific technology or device [13]. *Network Infrastructure* refers to devices such as switches and routers that enable data flow. The *Mobile Device* sub-class refers to hand held tablets, or smart phones. The *Computer Systems* class includes external (e.g. web) and internal (e.g. application) as well as personal computers.

### *2.7 Vulnerability*

The *Vulnerability* refers to the technical weakness exploited by the Attacker. This class is also exhaustively developed and defined by the CAPEC group, but only the following sub-classes are used in this paper: Configuration, Design and Human weakness [14]. *Configuration* vulnerabilities are initiated by incorrect configuration of a device or software. *Design* vulnerabilities occur due to a design error. Design errors can be in the protocol or in access control. *Human weakness* refers to the case where a human is manipulated to compromise the system, thus where the failure is not in the system but in its operator.

### *2.8 Scenario*

The final class is the *Scenario* class. These scenarios are used to classify cyber attacks [15]: Denial of Service, Web Defacement and Unauthorised Access. *Denial of Service* is defined as “attempts to prevent legitimate users from accessing information or services” [16]. *Web Defacement* refers to vandalism of a publicly available website [17]. *Unauthorised Access* is further divided into Financial Theft, Stealing Secrets and Changing Data.

*Financial Theft* refers to stealing money via computers. *Stealing Secrets* refers to curious or malicious individuals, spies, or anyone obtaining data that is not publicly available. Finally, *Changing Data* refers to unauthorised personnel or hackers gaining user rights to system or data flows and changing data with malicious intent.

### *2.9 Visual Representation*

These classes and subclasses are mapped onto a graph with three axes, each representing a sub-class. The plane that the marker is drawn on indicates the sub-classes of the attack. The position on that plane indicates the level of confidence of the attack in that specific sub-class. By allowing classes and sub-classes to be presented within a plane on three axes, this representation is superior to traditional approaches, which only classify elements into a single class or subclass.

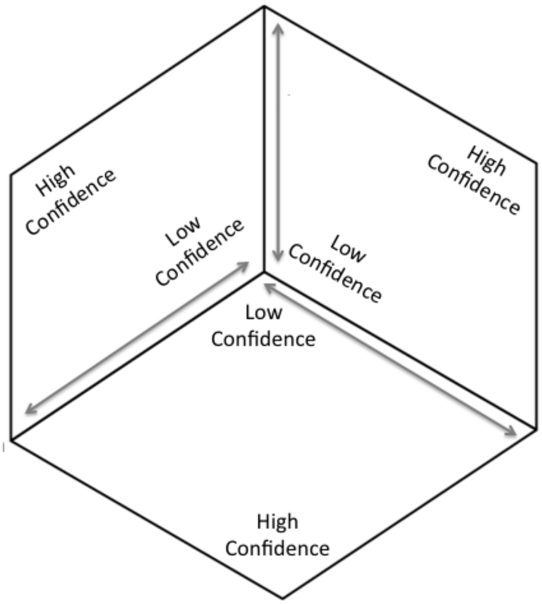


*Figure 1: Axes and planes for the visual representation*

## 3. Timeline

This section discusses a number of cyber attacks that occurred in South Africa from 1994 to 2015. These attacks will be used in the classification scheme to show how they can be classified in a visual manner. (They were not empirically selected, but subjectively.)

### *3.1 1994: SA Election*

An unknown hacker attempted to sabotage South African election results by hacking the electoral system, which was thought to be impenetrable. The unknown hacker, who gained access to the Election Commission's computer in the early hours of 3 May 1994 to manipulate the vote counts of three political parties, was detected but never identified. This attack disrupted the counting process as the electronic count was suspended and the backup manual process was used which delayed the announcement of the results by two days. The attempted manipulation ultimately had no influence on the final result [17–19].

### *3.2 1998: Telkom*

A 15-year-old boy who hacked his way through all the security features of the South African telecommunications company – Telkom's – computer systems was arrested on 22 October 1998. Internal monitoring devices found evidence of the boy's online footprint and investigators continued to monitor his online activity until they could track him down to where the South African Police Service (SAPS) could arrest him. The boy was in a position to do major damage to the system, including transferring large amounts of money, but he did not manipulate any data[2] [21].

### *3.3 1999: SA Statistics*

The official South African statistics web page was defaced. This web site has a high international significance, since it provides consumer price index and gross domestic figure information. The defacement was aimed at Telkom again. Hackers claiming to be from "B1nary Outlawz" replaced the normal web page with the following tirade: "Telkom stop your...lame-ass monopoly or we will disconnect you" [21, 22].

### *3.4 2003: ABSA Bank*

A hacker gained access to the Internet banking profiles of unsuspecting ABSA clients and stole at least R530 000 ($31 500). By sending emails containing spyware, the attacker gained access to users' bank account details and PIN numbers. ABSA stated that this attack was unknown to them at the time and that it took them a number of days to figure out how the hacker operated. The problem with this scenario was that the bank's security was never breached, as the perpetrator attacked the ABSA clients' home computers to gain access to the bank accounts [23, 24].

### *3.5 2005: Mass Defacement*

A Moroccan hacker group, called "Team Evil", hacked and defaced 260 South African websites in what was called "the biggest hack attack in SA's history". The hackers claimed responsibility for these attacks by posting political messages on the home pages of the hacked websites. After investigations it was determined that a single Internet service provider, named Gamco, hosted all the defaced websites. Gamco's director admitted that one of the servers were vulnerable, but was fixed as soon as the problem was identified [25, 26].

### *3.6 2010: LandBank*

During Christmas Eve of 2010, hackers attempted to steal R150 million ($9 million) from the South African LandBank. The LandBank is South Africa's agricultural finance house also known as The Land and Agricultural Development Bank of South Africa. The hackers used LandBank passwords, which they obtained by hacking into the bank's IT system though the help of insiders. Suspicious transfers were detected by anther South African Bank, ABSA, and they were able to prevent the theft in its initial stages. LandBank was able to recover all except about R 400 000 ($ 24 000) of their money [28].

### *3.7 2011: Spyphone*

A millionaire businessman illegally intercepted his estranged wife's e-mail, SMSes and other electronic messages. His actions were discovered in the divorce proceedings where he had access to suspect information. Spyware was then discovered on his wife's smart phone, which enabled communication monitoring, location tracking and eavesdropping. Related to this, the information of 175 000 South African users of the adultery web site Ashley Madison, was leaked in 2015 [28, 29].

[2] http://www.cellular.co.za/news_1998/news-telkom_hack.htm

### *3.8 2011: ANCYL*

The African National Congress Youth League's (ANCYL) web site was defaced multiple times during the period between March 2011 and August 2011. In the first defacement, the then leader of the Youth League, Julius Malema, was reported on their web site as stating: “After much thought I, Julius Malema, have decided to step down as ANC Youth League President.” and “I have brought my party the ANC into disrepute (sic); I have disrespected my elders and have made a fool out of myself; I promote my own agenda over my country and parties; I promote the singing of racist songs to promote violence and unrest in the country”. The group “Blah Blah protest group” took responsibility for the defacement. Figure 2 shows an image of the defaced website [30–34].

The main ANC group has also been a target of hacker. In December 2015 the ANC twitter account was compromised and false tweets stating that President Jacob Zuma has been recalled. A screenshot of this tweet is shown in Figure 3 [36].

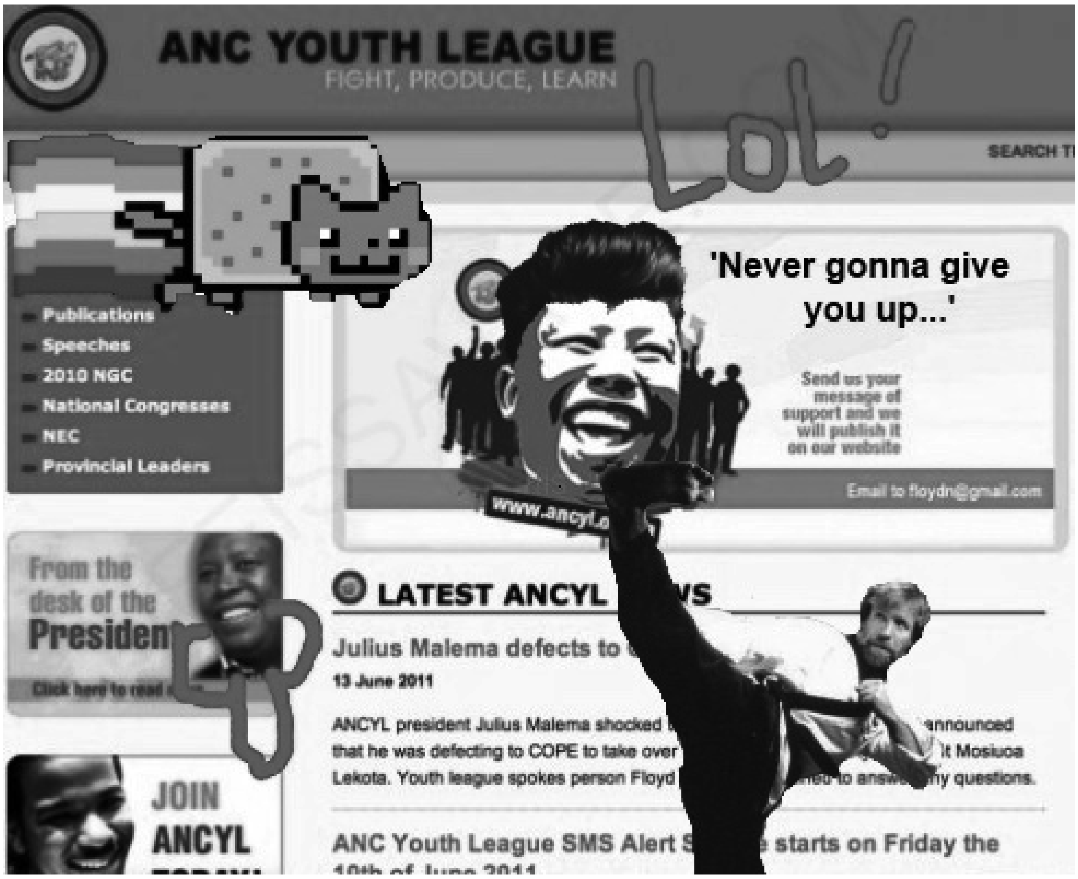
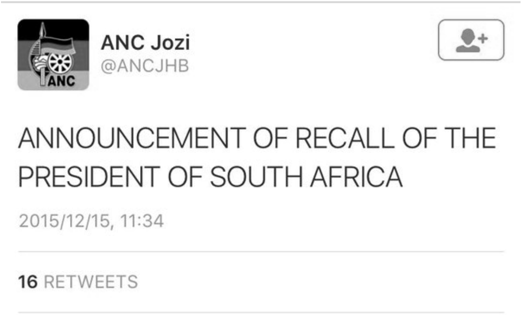

ANC YOUTH LEAGUE
FIGHT, PRODUCE, LEARN
Lol!
SEARCH T
Publications
Speeches
2010 NGC
National Congresses
NEC
Provincial Leaders
'Never gonna give you up...'
Send us your message of support and we will publish it on our website
Email to floydn@gmail.com
www.ancyl.o
From the desk of the President
Click here to read
LATEST ANCYL NEWS
Julius Malema defects to
13 June 2011
ANCYL president Julius Malema shocked announced that he was defecting to COPE to take over it Mosiuoa Lekota. Youth league spokes person Floyd to answer my questions.
ANC Youth League SMS Alert starts on Friday the 10th of June 2011
JOIN ANCYL TODAY!

*Figure 2: ANCYL website defacement*


ANC Jozi
@ANCJHB

ANNOUNCEMENT OF RECALL OF THE PRESIDENT OF SOUTH AFRICA

2015/12/15, 11:34

**16** RETWEETS

*Figure 3: ANC Jozi Tweet*

### *3.9 2012: PostBank*

A hacker stole R42 million ($2.5 million) from the South African PostBank. This hack was also performed during the Christmas break where a Postbank employee used the computer of a colleague who was on holiday. This computer was linked to the PostBank main server, from which he could to transfer money. Money was withdrawn from various ATM's throughout South Africa. Two criminals, Motsoane and Masoleng, were arrested in February 2012 and both sentenced to 15 years in jail [36, 37].

### *3.10 2013: IOL DDoS*

Anonymous Africa claimed responsibility for launching a Distributed Denial of Service (DDoS) attack on the Independent Newspaper web site iol.co.za. The attack was in response to claims that the IOL group supports Zimbabwean president Robert Mugabe. The following taunt was sent to boast about the attack: "IOL bad boys bad boys what you ganna do, what you ganna do when they come for you". The attack was able to disrupt the web site for about a day [38, 39].

### *3.11 2014: Mr Price*

Mr Price, a South African clothing store, was able to avert a conman from accessing the account of a Mr Thompson. Mr Thompson's cell phone account was already in the conman's control. What is unique to this attack, is that a recording of the call is available online[3]. The call centre agent detected the attempted fraud and prevented any additional damage to Mr Thomson [41].

### *3.12 2015: State Security Agency Spy Cables*

The Al Jazeera's news agency obtained leaked cables from the South African State Security Agency from 2006 to 2014 [42]. They published selected excerpts which revealed a number of security flaws and lapses within the South African government and intelligence services [43]. The documents were leaked by an intelligence agent who allowed his brother-in-law to access his official computer [44]. As a consequence of this leak, several South African intelligence agents (spies) had to be withdrawn [45].

A timeline of these events is presented in Figure 4.

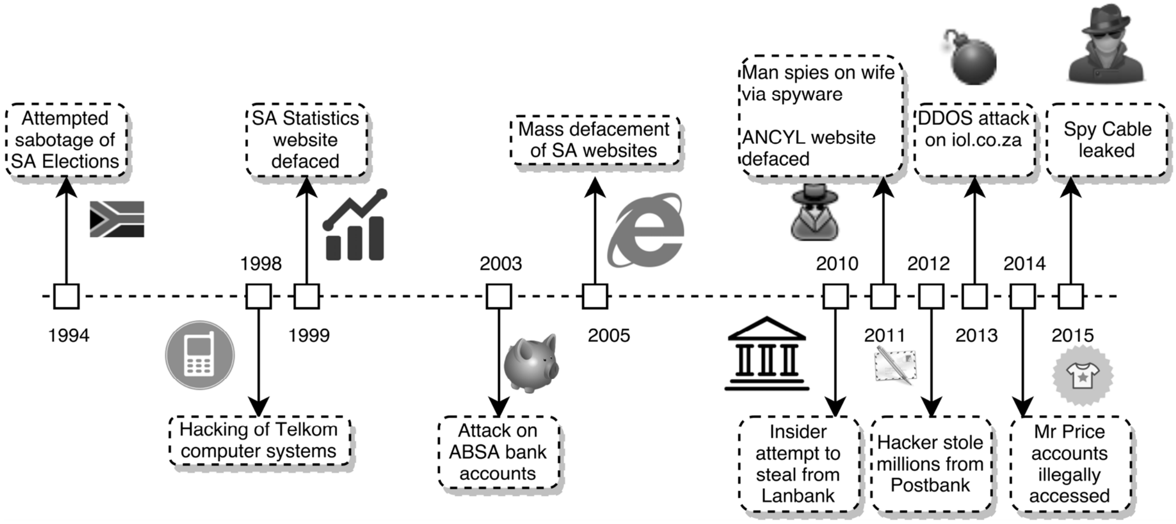

Attempted sabotage of SA Elections
SA Statistics website defaced
Mass defacement of SA websites
Man spies on wife via spyware
ANCYL website defaced
DDOS attack on iol.co.za
Spy Cable leaked
1994
1998
1999
2003
2005
2010
2011
2012
2013
2014
2015
Hacking of Telkom computer systems
Attack on ABSA bank accounts
Insider attempt to steal from Lanbank
Hacker stole millions from Postbank
Mr Price accounts illegally accessed

*Figure 4: Timeline of Attacks*

[3] https://www.youtube.com/watch?v=2FFPvBU7VYo

## 4. South African Cyber Attack Classification

The various cyber attacks discussed in the timeline are classified according to the method introduced in Section 2. For each classification, an analysis is presented to show the diversity of the impact of attacks in South Africa. All twelve attacks are sorted according to each class and presented visually. The graphs features three axes, each indicating the sub-classes and how well each attack falls into each sub-class. Each attack is represented by a marker to reveal the confidence in its classification.

### *4.1 Attacker*

This classification looks at the entity that performed the attack. As mentioned earlier, the attacker may fall into more than a single sub category. Figure 5 shows the Attacker graph.

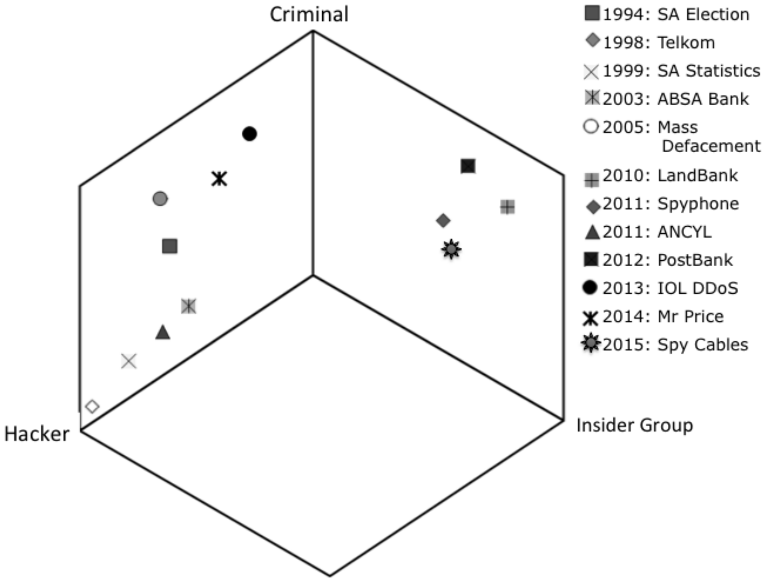


*Figure 5: Attacker Classification Graph*

It can be seen that most of the attackers in the featured cyber attacks were hackers as they broke through a company's defences illegally to perform their attack, except for the cases where insiders were present. In addition, the presence of insider information and spyware enabled the attacker to gain access to the target system without the need for breaking through the organisations' defences. Lastly, it can be seen that all of the attackers are classified as having criminal intent, except for the young boy who hacked into Telkom's system “just to see if he can”.

### *4.2 Goal*

Next, we examine the intent behind the various attacks. Criminal activities can have multiple motives, which include stealing, disrupting or changing data. The Goal classification graph is shown in Figure 6.

From the figure, it can be seen that the purpose of attack is highly scattered. This shows that a range of objectives drove the various cyber attackers. This classification clearly groups certain attacks together. All the attacks relating to financial gain (stealing money from banks or accounts) are classified in the sub-classes of Stealing as well as Changing Data. The defacement incidents are classified in the Changing Data sub-class, as well as the Disrupting sub-class.

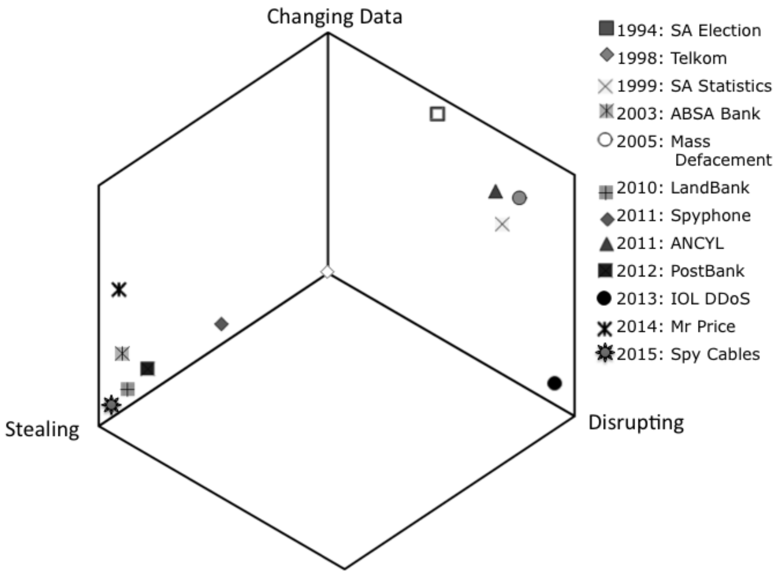


*Figure 6: Goal Classification Graph*

It is clear to understand why no cyber attacks fall in the sub-classes Stealing and Disrupting as the action of stealing normally goes hand-in-hand with being stealthy and going unnoticed. The most interesting case again is the young hacker who broke into Telkom's computer system, who seemed to have no intent of stealing, altering data or disrupting the services.

### 4.3 Mechanism

The Mechanism classification relates to the method of attack. The Mechanism classification graph is shown in Figure 7. In this classification, most of the cyber attacks are grouped together. The cyber attacks that include defacement of websites and attacking of banking systems, fall into the sub-classes of Information Gathering and System Abuse. In all of these cases, the system of the target was abused in order to achieve their goal, which could be stealing, disrupting or the changing of data, as discussed in the Goal classification.

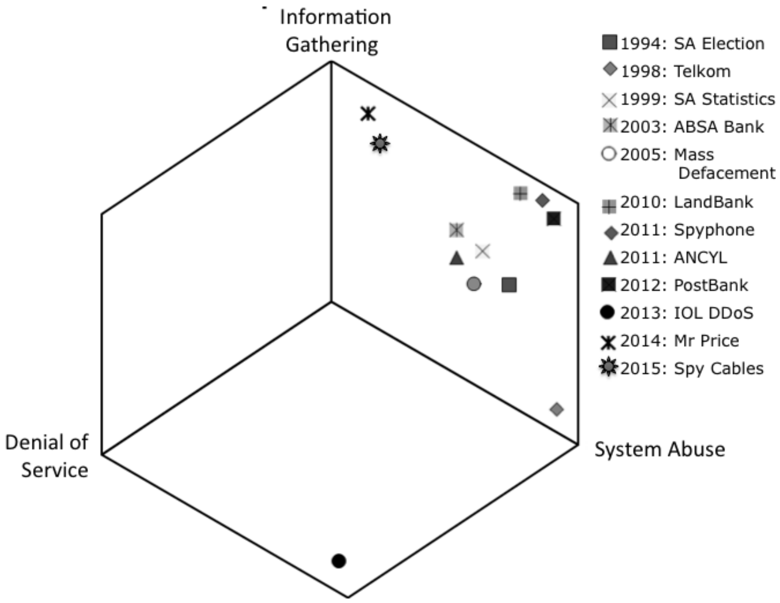


*Figure 7: Mechanism Classification Graph*

The exception of these attacks is the DDOS attack on the iol.co.za website. The clear divide can be seen between a Denial of Service attack and the other two subclasses, as a successful Denial of Service attack would make information gathering and further system abuse extremely difficult.

### *4.4 Effect*

The Effect classification clarifies the impact of the attack. Per definition of Minor, Major and Critical, each cyber attack can only fall into one of the three categories, thus displayed on the axis of the graph. The Effect classification graph is shown in Figure 8. In this graph, the clear groupings of the cyber attacks can be observed. The website defacement and attacks that were discovered are classified in the Minor sub-class. All the attacks on Financial Institutions are classified as Major Effect as a part of the money stolen in each case was not recovered.

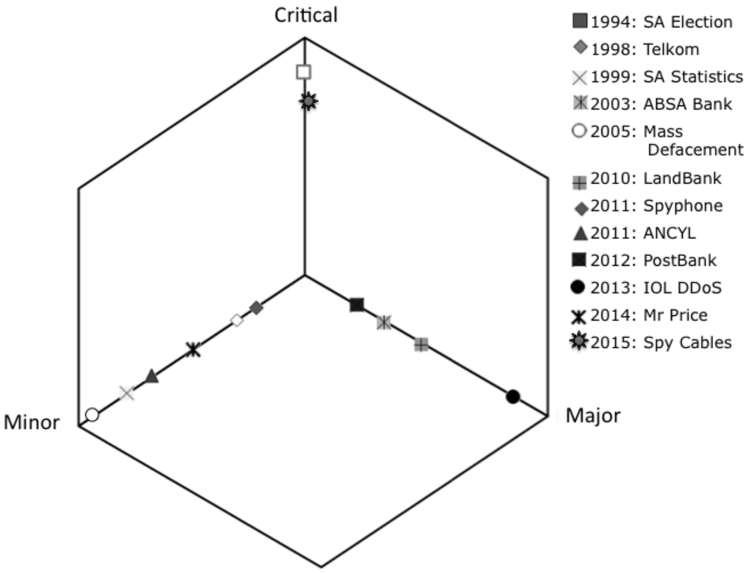


*Figure 8: Effect Classification Graph*

The sabotage of the 1994 electronic election system caused the system to be abandoned and the Electoral Commission to revert to manual counting, therefore it is classified as an attack with Critical Effect. The leaked Spy Cables could place intelligence agents in danger and are therefore also classified as Critical [45].

### *4.5 Motivation*

The Motivation class considers why the attacker performed this attack. The sub-classes include Political, Criminal/Financial or Fun/Personal motivation. The Motivation classification graph is shown in Figure 9. From the Motivation classification graph, it can be seen that all the attempts at stealing money or personal information can be grouped in the Criminal/Financial and Fun/Personal sub-classes as they were all performed for personal gain. The website defacement attacks are classified in the Political and Fun/Personal sub-classes as all the defacement attacks were motivated by political or service delivery issues. The exception, again, is the young hacker whose attack was solely motivated by Fun.

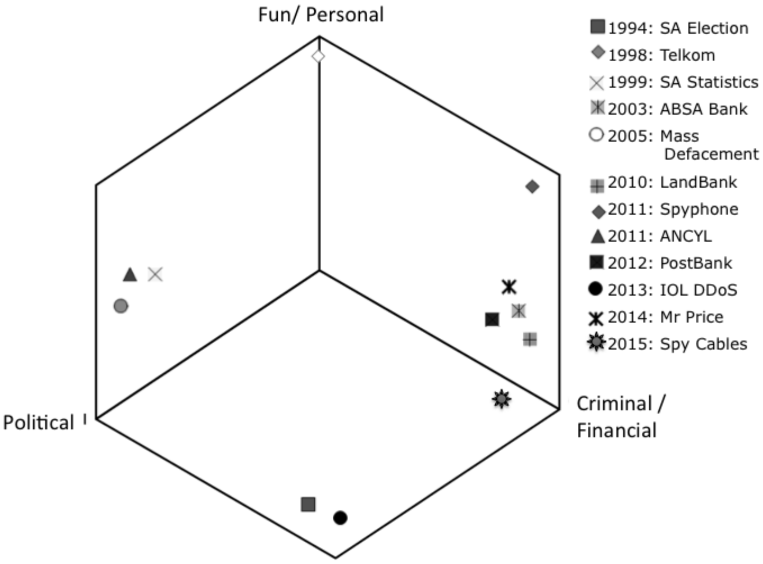


*Figure 9: Motivation Classification Graph*

## *4.6 Target*

The Target category focuses on the devices that were targeted during the cyber attack. The Target classification graph is shown in Figure 10. It can be seen from the graph that in most cases, the Target of the attacker was either the computer system or the network infrastructure devices. The exception to this is the attacks where mobile phones were used to gain access or information to in order to launch the attack.

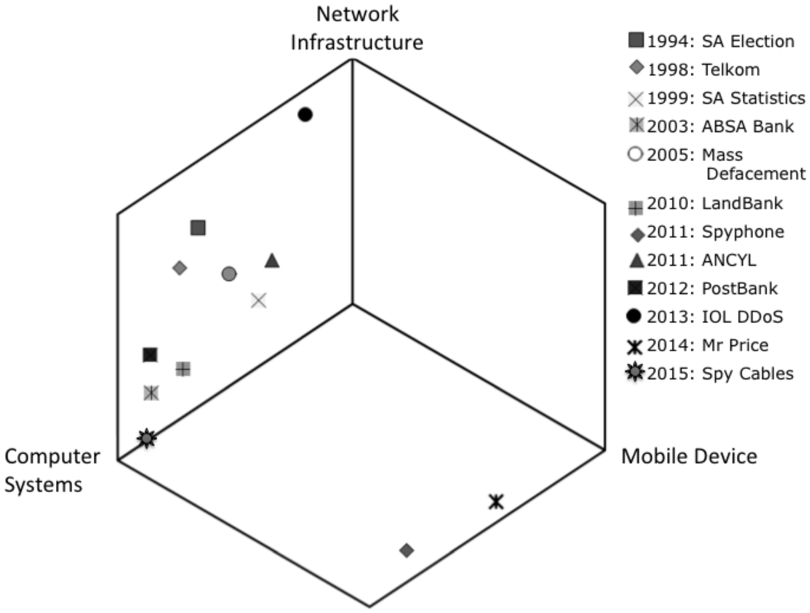


*Figure 10: Target Classification Graph*

## *4.7 Vulnerability*

The Vulnerability classification considers the weakness that was exploited by the attacker. This graph is shown in Figure 11. In this classification, a clear grouping of attacks can be seen. All the attacks where insiders were involved, and where malicious software was installed on victim's phones or computers, fall in the Human Weakness sub-class. The cyber attacks where systems were hacked with no assistance from insiders or installed malicious software fall in the Configuration and Design sub-classes, as the targeted systems were not secure.

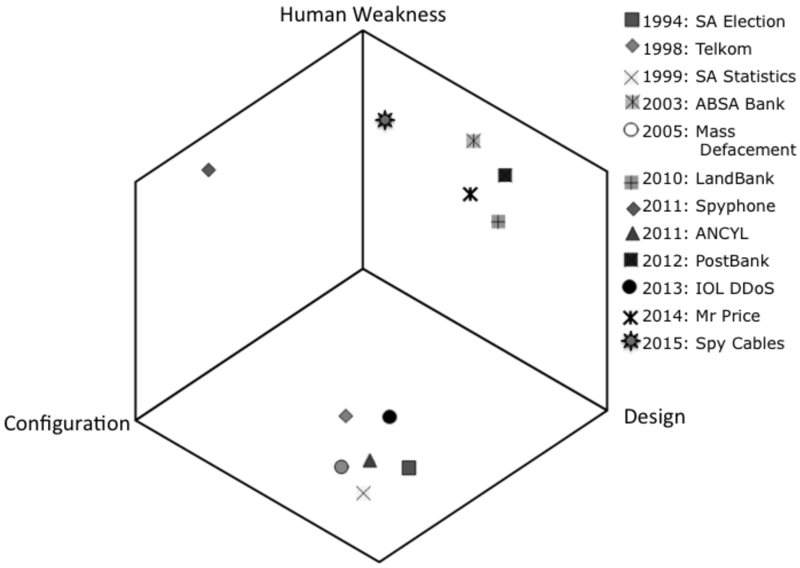


*Figure 11: Vulnerability Classification Graph*

### 4.8 Scenario

The final class places the attack in a cyber attack category. As an attack only falls within one category, all the markers are presented on the axis of the graph. As the Unauthorised Access Scenario class can be divided into a further three subclasses, the division is indicated on the same graph for clarity purposes. The Scenario classification graph and the further sub-class divisions are shown in Figure 12. All the web defacement attacks fall under the Web Defacement sub-class and all the Denial of Service attacks under the Denial of Service sub-class. The Unauthorised Access sub-class contains all the attacks where a hacker gained access to the system for stealing money, information or the changing of data. This classification relates to the Goal classification, which considers Stealing, Disrupting and Changing Data.

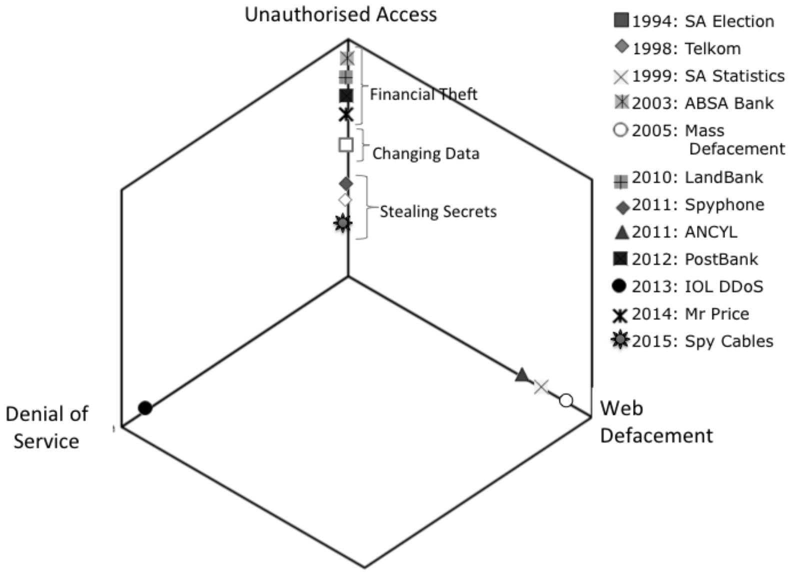


*Figure 12: Scenario Classification Graph*

## 5. Discussion

In this paper, twelve cyber attacks were classified to identify the impact of the attacks. These classifications considered the goal, target, motivation and other factors relating to cyber attacks in general. Through the classification of each cyber attack, the impact of an attack can be determined, trends can be analysed and the incidents can be compared in a logical manner. These classifications can be used for any type of attack to answer questions such as:

- Who performed the attack?
- What did they want to achieve?
- How did they do it?
- What damage did they cause?
- Who did they target?
- What did they exploit?
- Finally, in what category can this attack be categorised?

This classification scheme is useful as incidents and attacks can be classified according to various characteristics. The division into various classes and sub-classes enables the user to compare various incidents with other incidents from his/her team or other response teams. This enables the user to do the following:

1. Identify the impact and risk of the attack or incident
2. Compare Cyber attacks
3. Find trends
4. Respond in the appropriate fashion after the incident.

For example, when an incident resulting from an attack is reported, the first responder can classify the attack according to the classes provided and through visual analysis determine if there existed similar attacks in the past. This will provide a quick overview for the responder to determine what the right course of action is to respond to this attack. To illustrate the how different stakeholder groups will benefit from the use of such a classification model, two brief use cases will be discussed. In both use cases, three or four of the incidents discussed in Section 3 will be selected and compared to try and identify a possible trend that can be useful.

*Use Case 1: Website Attacks*

Websites are a common communication medium for companies, organisations and individuals. Attacks on these websites can restrict or stop the normal operations of these companies. Research can be done on the trends of website attacks in order to better understand and prepare against these types of cyber attacks. The four website attacks to be studied are:

- 1999: SA Statistics website defacement
- 2005: Mass defacement of SA websites
- 2010: ANCYL website defaced
- 2013: DDOS attack on iol.co.za

When analysing the classification of these four attacks done in Section 4, the following can be deduced:

1. All the attacks were performed by politically motivated hacker/criminal groups with a goal to disrupt or change presented information by attacking the network infrastructure of computer systems.
2. The impact of website defacement attacks is minor, but the DDOS attacks launched in the one case had a much larger impact.

3. Website attacks are not a new type of attack in South Africa. The attacks took place over a course of approximately 15 years spaced 3-5 years apart.

It can be deduced that any insecure website can be targeted by political motivated groups, not only the websites of the institutions directly associated political actions. It can also be seen that it is critically important to secure your network infrastructure and computer systems against any possible attacks. Although website defacement can disrupt normal operations, attacks such as a DDOS can have a greater impact and protection against these attacks is extremely important.

*Use Case 2: Attack on financial institutions*

Every bank has network and computer infrastructure which must be secured against malicious activity. Attacks on this infrastructure can lead to a loss of millions of Rands. Research can be done on the trends of attacks on financial institutions in order to better understand and prepare against these types of cyber attacks. The three attacks on financial institutions to be studied are:

- 2003: Attack on ABSA bank Accounts
- 2010: Insider attempt to steal from Landbank
- 2012: Hacker stole millions from Postbank

When analysing the classification of these three attacks done in Section 4, the following can be deduced:

1. One attack was launched by a criminal/hacker who collected client information where the two other attacks were launched by obtaining information from employees.
2. The exploitation of human weakness (clients and employees) made detection difficult, which caused major damage to the institutions.

It can be deduced that the biggest threat to financial institutions relating to the analysed cyber attacks is the exploitation of human weakness. These institutions can have excellent computer and network security, but they need to ensure that the employees can be trusted.

These two use cases are done in retrospect, but can also be done right after an attack is detected. When an incident of an attack is reported, the first responder can classify the attack according to the classes provided and through visual analysis determine if there existed similar attacks in the past. This will provide a quick overview for the responder to determine what the right course of action is to respond to this specific attack.

## 6. Conclusion

The integration of IT in our daily lives has created an environment where unreliable or insecure systems can cause major financial, environmental, social, political or personal damage. This paper introduced a cyber attack classification scheme that can assist the user to compare cyber attacks, find trends, determine the impact thereof and plan a possible course of action. An advantage of this classification scheme is that the results can be represented in visual form.

To illustrate the usefulness of this scheme, the paper considered twelve of the most prominent cyber attacks in South Africa over the past 22 years (1994-2015) and classified them in order to show the diverse impacts of these cyber attacks in South Africa. This classification process maps attacks graphically to visually present various aspects of the attack. By classifying attacks visually, temporal and other patterns can be quickly deduced.

To illustrate how different stakeholder groups will benefit from the use of such a classification model, two use cases were presented. These showed how this classification model can be used to analyse attacks, determine the impact as well as identify possible trends. It can be seen from the two use cases, that various attacks can easily be compared and valuable information can be obtained.

Future research could include the mapping of more attacks (perhaps with global diversity) as well as investigation of a method to automate the classification. The Mechanism, Target and Vulnerability classes can be automated by current intrusion detection tools/systems. The Motivation and Goal classes are difficult to automate because of the subjective nature of the classes. By mapping events on a plane rather than into a single class, future research into the automation of the classification process can be enhanced.

## References

[1] MITRE, "Common Attack Pattern Enumeration and Classification," 2016. [Online]. Available: https://capec.mitre.org/.

[2] R. van Heerden, L. Leenen, B. Irwin, and I. Burke, "A computer network attack taxonomy and ontology," *Int. J. Cyber Warf. Terror.*, vol. 3, pp. 12–25, 2013.

[3] R. P. van Heerden, I. D. Burke, and B. Irwin, "Classifying Network Attack Scenarios Using an Ontology," in *Proceedings of the 7th International Conference on Information-Warfare & Security (ICIW 2012)*, 2012, pp. 311–324.

[4] M. Rounds and N. Pendgraft, "Diversity in network attacker motivation: A literature review," in *2009 International Conference on Computational Science and Engineering*, 2009, pp. 319–323.

[5] G. B. Magklaras and S. M. Furnell, "Insider threat prediction tool: Evaluating the probability of IT misuse," *Comput. Secur.*, vol. 21, no. 1, pp. 62–73, 2001.

[6] A. Simmonds, P. Sandilands, and L. van Ekert, "An ontology for network security attacks," *Appl. Comput.*, no. 2, pp. 317–323, 2004.

[7] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework," in *Information Security for South Africa (ISSA), 2014*, 2014, pp. 1–9.

[8] B. Krebs, "The Scrap Value of a Hacked PC, Revisited," Oct-2012. [Online]. Available: http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/.

[9] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, 2004.

[10] R. P. Van Heerden, B. Irwin, I. D. Burke, and L. Leenen, "A computer network attack taxonomy and ontology," *Int. J. Cyber Warf. Terror.*, vol. 2, no. 3, pp. 12–25, 2012.

[11] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante, "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," *Technol. Soc. Mag. IEEE*, vol. 30, no. 1, pp. 28–38, 2011.

[12] H. Orman, "The Morris worm: A fifteen-year perspective," *IEEE Secur. Priv.*, no. 5, pp. 35–43, 2003.

[13] F. Mouton, L. Leenen, M. M. Malan, and H. S. Venter, "Towards an ontological model defining the social engineering domain," in *ICT and Society*, Springer Berlin Heidelberg, 2014, pp. 266–279.

[14] S. Hansman and R. Hunt, "A Taxonomy of Network and Computer Attack Methodologies," Department of Computer Science and Software Engineering University of Canterbury, 2003.

[15] R. van Heerden, L. Leenen, and B. Irwin, "Using an Automated Reasoner to Classify Computer Network Attacks," in *5th Workshop on ICT Uses in Warfare and the Safeguarding of Peace*, 2013.

[16] M. McDowell, "Understanding Denial-of-Service Attacks," Nov-2009. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-015.

[17] N. Balakrishnan and M. Sarma, "A Perspective On The Social Cognition Of Hacker Groups And The Multi Dimensional Aspects Of Web Defacements: A Fused Analysis," 2004.

[18] A. Laing, "Election won by Mandela 'rigged by opposition,'" Oct-2010. [Online]. Available: http://www.telegraph.co.uk/news/worldnews/africaandindianocean/southafrica/8084053/Election-won-by-Mandela-rigged-by-opposition.html.

[19] J. Leyden, "Hacker almost derailed Mandela election in South Africa," Oct-2010. [Online]. Available: http://www.theregister.co.uk/2010/10/27/sa_election_hack/.

[20] M. Plaut, "Book says hacker tried to stop Mandela coming to power," Oct-2010. [Online]. Available: http://www.bbc.com/news/world-africa-11630092.

[21] W. Knowles, "South Africa police arrest teen hacker," 1998. .

[22] S. Xako, "Africa: Hackers deface Stats SA website with obscenities," Dec-1999. [Online]. Available: http://allafrica.com/stories/199912060109.html.

[23] Hellkom, "Hackers Deface stats website," 1999. [Online]. Available: http://www.hellkom.co.za/news/local/page-579.

[24] J. Thorpe, "Absa hacker saga encourages better IT security," Aug-2003. [Online]. Available:

http://www.itweb.co.za/index.php?option=com_content&view=article&id=78132.

[25] L. Altenroxel and G. Thiel, “How ABSA hacker targeted clients’ home PCs,” 2003. [Online]. Available: http://www.iol.co.za/news/south-africa/how-absa-hacker-targeted-clients-home-pcs-1.110109.

[26] L. Mbongwa and J. Makua, “Moroccan hackers blamed for website blitz,” 2005. [Online]. Available: http://www.iol.co.za/moroccan-hackers-blamed-for-website-blitz-1.231419.

[27] Buys_Inc_Attorneys, “Biggest Hack Attack in SA’s History,” 2005. .

[28] D. Potgieter, “Absa intercepts Land Bank swindle,” 2011. [Online]. Available: http://www.iol.co.za/business/companies/absa-intercepts-land-bank-swindle-1.1009423.

[29] J. Vermeulen, “Ashley Madison hack list: South African details,” *Mybroadband*, 2015. [Online]. Available: http://mybroadband.co.za/news/security/135972-ashley-madison-hack-list-south-african-details.html.

[30] M. Laganparsad, “Man probed for spying on wife,” 2011. [Online]. Available: http://www.timeslive.co.za/local/2011/11/27/man-probed-for-spying-on-wife.

[31] B. Huisman, “ANCYL website hacked,” 2011. [Online]. Available: http://www.timeslive.co.za/politics/2011/03/31/ancyl-website-hacked.

[32] K. Redelinghuys, “ANC Youth League website hacked by Warbird,” 2011. [Online]. Available: http://memeburn.com/2011/03/anc-youth-league-website-hacked/.

[33] Savage, “The ANCYL says its website was tampered with and Juju is still a part of it [pic],” 2011. [Online]. Available: http://lifeissavage.com/2012/05/03/the-ancyl-says-its-website-was-tampered-with-and-juju-is-still-a-part-of-it-pic/.

[34] S. Thomas, “ANC Youth League website hacked,” 2011. [Online]. Available: http://memeburn.com/2011/07/anc-youth-league-website-hacked-2/.

[35] R. Muller, “ANC Youth League website hacked again,” 2011. [Online]. Available: http://mybroadband.co.za/news/internet/32556-anc-youth-league-website-hacked-again.html.

[36] M. Winsor, “South Africa ANC Twitter Hack: President Jacob Zuma Not Removed From Office, African National Congress Says,” *International Business Times*, 2015. [Online]. Available: http://www.ibtimes.com/south-africa-anc-twitter-hack-president-jacob-zuma-not-removed-office-african-2225917.

[37] W. Swart and M. Afrika, “It was a happy New Year’s Day for gang who pulled off R42m Postbank heist,” 2012. [Online]. Available: http://www.timeslive.co.za/local/2012/01/15/it-was-a-happy-new-year-s-day-for-gang-who-pulled-off...r42m-postbank-heist.

[38] W. Swart, “‘Inside man’ who sank R30m heist,” 2012. [Online]. Available: http://www.timeslive.co.za/sundaytimes/2012/09/23/inside-man-who-sank-r30m-heist.

[39] R. Stein, “Hacktivists ‘Anonymous Africa’ attack SA news site IOL,” 2013. [Online]. Available: http://memeburn.com/2013/06/hacktivists-anonymous-africa-attack-sa-news-site-iol/.

[40] L. Antony, “Hackers shut down IOL’s website, e-mail,” 2013. [Online]. Available: http://www.iol.co.za/dailynews/news/hackers-shut-down-iols-website-e-mail-1.1531701.

[41] J. Vermeulen, “SA scammer caught in action,” 2014. [Online]. Available: http://mybroadband.co.za/news/banking/100018-sa-scammer-caught-in-action.html.

[42] Al Jazeera Investigative Unit, “The Spy Cables: A glimpse into the world of espionage,” *Al Jazeera Africa*, 2015. [Online]. Available: http://www.aljazeera.com/news/2015/02/spy-cables-world-espionage-snowden-guardian-mi6-cia-ssa-mossad-iran-southafrica-leak-150218100147229.html.

[43] R. Polak, “Whither the Whistleblower: Who leaked the Spy Cables, and why?,” *Daily Maverick*, 2015. [Online]. Available: http://www.dailymaverick.co.za/article/2015-02-25-whither-the-whisteblower-who-leaked-the-spy-cables-and-why/.

[44] S. Maphumulu, “Apartheid spook ‘sold secrets,’” *Independent Online*, 2015. [Online]. Available: http://www.iol.co.za/news/politics/apartheid-spook-sold-secrets-1.1828648.

[45] M. Ispas, “Spy Cables: SA Spies Extracted From Posts,” *SA Breaking News*, 2015. [Online]. Available: http://www.sabreakingnews.co.za/2015/03/02/spy-cables-sa-spies-extracted-from-posts/.