Pro-active visualization of cyber security on a National Level: A South African Case Study

Submitted in fulfillment
of the requirement of the degree of

DOCTOR OF PHILOSOPHY

of Rhodes University

Ignatius Petrus Swart

Grahamstown, South Africa

January 2015

Abstract

The need for increased national cyber security situational awareness is evident from the growing number of published national cyber security strategies. Governments are progressively seen as responsible for cyber security, but at the same time increasingly constrained by legal, privacy and resource considerations. Infrastructure and services that form part of the national cyber domain are often not under the control of government, necessitating the need for information sharing between governments and commercial partners. While sharing of security information is necessary, it typically requires considerable time to be implemented effectively. In an effort to decrease the time and effort required for cyber security situational awareness, this study considered commercially available data sources relating to a national cyber domain. Open source information is typically used by attackers to gather information with great success. An understanding of the data provided by these sources can also afford decision makers the opportunity to set priorities more effectively.

Through the use of an adapted Joint Directors of Laboratories (JDL) fusion model, an experimental system was implemented that visualized the potential that open source intelligence could have on cyber situational awareness. Datasets used in the validation of the model contained information obtained from eight different data sources over a two year period with a focus on the South African .co.za sub domain. Over a million infrastructure devices were examined in this study along with information pertaining to a potential 88 million vulnerabilities on these devices. During the examination of data sources, a severe lack of information regarding the human aspect in cyber security was identified that led to the creation of a novel Personally Identifiable Information detection sensor (PII). The resultant two million records pertaining to PII in the South African domain were incorporated into the data fusion experiment for processing. The results of this processing are discussed in the three case studies. The results offered in this study aim to highlight how data fusion and effective visualization can serve to move national cyber security from a primarily reactive undertaking to a more pro-active model.

Acknowledgements

David Brin in his book "*A long lonely road, advice to new writers*" stated that studying for a PhD is an extremely isolating experience. This is certainly true to a certain extent but it would be foolish of me to consider that I completed this study on my own. Attempting to balance family and a full time career while studying took considerable effort, not all of it from me. For that reason I have a number of singular individuals to thank, starting with my lovely wife Reinette. The late hours I spent working on my experiment, publications or thesis was not always achieved in balance. Thank you for your patience and understanding during this lengthy process. I will honor our agreement to not study anything formally for at least a year upon completion of this degree.

Both my study leaders Prof Barry Irwin and Prof Marthie Grobler deserve a special thank you. They not only contributed significantly to the content of this study but served as inspiration right from the start. Prof Irwin's work on data collection and visualization at an organizational and international level, raised my aspirations for my own research. Prof Grobler's work on national strategies and standards instilled in me a deep appreciation for the effort it takes to create structure where there is none. Thank you both for your guidance and inspiration.

Funding for this work was in part received from the Council for Scientific and Industrial Research (CSIR) and for that I thank them. A large number of open source applications and open access datasets were used as resources in this study. Without the availability of these open source resources, a considerable amount of time would have been spent re-creating the components required for such a system. A full list of open source resources used is available in Chapter 4 and Appendix C. A special thank you to Pieter, Priaash, Shazia, Alex and Johnny, who have taken availability of information to new heights in their various software implementations.

Others not specifically mentioned who will never read (or care to understand) this, but still played a important part: Thank you to my friends, mom, and of course my ever patient listening dog.

Content

List of Figures

List of Tables

List of acronyms

Acronym	Description
AFRINIC	African Network Information Center
ALE	Annualized Loss Expectancy
API	Application Programming Interface
ARO	Annualized Rate of Occurrence
ASN	Autonomous System
ASR	Asset Summary Reporting
BGP	Border Gateway Protocol
C&C	Command and Control
CCE	Common Configuration Enumeration
CERT	Computer Emergency Readiness Team
CIRT	Computer Incident Response Team
CMS	Content Management System
CSIRT	Computer Security Incident Response Team
CSRF	Cross Side Request Forgery
CSS	Cascading Style Sheet
CVE	Common Vulnerabilities and Exposures
CVRF	Common Vulnerability Reporting Framework
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CWRAF	Common Weakness Risk Analysis Framework
CWSS	Common Weakness Scoring Systems
CYBOX	Cyber Observable Expression
DARPA	Defense Advanced Research Project Agency
DNS	Domain Name System
ECT	South African Electronic Communications and Transactions Act
ENISA	The European Union Agency for Network and Information Security
ERD	Entity Relationship Diagram
EW	Electronic Warfare
GDP	Gross Domestic Product
GIS	Geographic Information System
HCI	Human Computer Interaction
HUMINT	Human Intelligence

ICT	Information and Communication Technology
IDS	Intrusion Detection System
IOC	Indicators Of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
JDL	Joint Directors of Laboratories
JSON	JavaScript Object Notation
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
OSINT	Open Source Intelligence
OSVDB	Open Source Vulnerability Database
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PC	Personal Computer
PDCA	Plan Do Check Approach
PHI	Personal Health Information
PII	Personally Identifiable Information
POC	Proof Of Concept
POPI	South African Protection of Personal Information Act
reCAPTCHA	re-Completely Automated Public Turing test to tell Computers and Humans Apart
RFID	Radio Frequency Identification
RIPE NCC	The Réseaux IP Européens Network Coordination Centre
RSA	Republic of South Africa
SA	Situational Awareness
SANS	System Administration, Networking and Security Institute
SAPS	South African Police Service
SCADA	Supervisory Control And Data Acquisition
SCRM	Supply Chain Risk Management
SLE	Single Loss Expectancy

SME	Small, Medium Enterprise
SMTP	Simple Mail Transfer Protocol
SOHO	Small Office Home Office
SSL	Secure Sockets Layer
STIX	Structured Threat Information Expression
TCP	Transmission Control Protocol
TTP	Tactics, Techniques and Procedures
UK	United Kingdom
uPNP	Universal Plug and Play
USA	United States of America

PART I

Introduction

It is straightforward to see the value of information sharing: as a matter of logic you cannot, for example, know whether you are a target of choice or a target of chance unless you compare your attack pressure to that of others.

D.E. Geer – Chief Information Officer, In-Q-Tel

1

Introduction

The quantity of information on the Internet is simply staggering and with the barrier to entry dropping lower and lower, more and more people are contributing. It is to this global collection of infrastructure that we increasingly entrust our personal information and data to achieve an improvement over the traditional way of conducting business. There is however the challenge of keeping this ever expanding Internet controlled in such a manner that it retains its ease of accessibility but still provides adequate protection to individuals and organizations. With no single governing body, a plethora of opinions on how to achieve safety, and technology moving at such a rapid pace that protection mechanisms become obsolete before they are really effective, it is not a trivial task. While technical solutions are widely available for nearly any possible information technology security challenge, few companies have the required personnel to fully utilize these solutions. Since the skills required to make use of the Internet has dropped considerably, many individuals and companies participate in the commercialization of information but lack the required understanding of security principles. Assigning blame for this lack of understanding is a complex discussion. Regardless of this, the only way to achieve security on a national level is with the co-operation of all entities involved, whether they are from private or government sectors. Any proposed solution to increase the state of information security has to bear in mind that not everyone is a information security specialist, nor do they want to be. The research presented will examine existing data sources related to cyber security, in order to highlight the potential effective information sharing could achieve.

1.1 PROBLEM STATEMENT

The attention given to Internet security has significantly increased in recent years. As many as 22% of people today consider security important, up from only 4% just a few years ago. It is shown that, in the event of a security incident, companies can expect a significant loss of customers, as much as 4.4% of customer base per incident (Ponemon Institute, 2013). Calculating the true cost of cyber crime is currently a contested topic of debate since it depends on the viewpoint of the individual performing the calculations (Anderson, Barton, Böhme, Clayton, van Eeten, Levi et al., 2013; Krausz & Walker, 2013). For example, should the cost of running anti-virus, anti-spam and firewall software be included in the calculations or should it be seen as general expenditure for organizations to participate on the Internet? (Zhura, 2013). As such the global annual cost of cyber crime is estimated between $575 billion and potentially as high as $1 trillion dollars (Center for Strategic and International Studies, 2014). Regardless of the cost, cybercrime is becoming so prevalent that it can be seen as the most common crime in modern society and as such it definitely requires urgent corrective measures (Anderson et al., 2013).

Vulnerabilities in infrastructure has always existed, but what sets information security vulnerabilities apart is the fact that the potential to exploit the vulnerability is available to anyone with a Internet connection (Yang, Stotz, Holsopple, Sudit & Kuhl, 2009). Since governments are seen as being responsible for a nation's safety (Broadhurst, 2006), the increase of cyber crime has increasingly put governments under pressure to address the fragility of Internet security. To address the requirement, a multitude of legislation, frameworks and structures have been developed to address vulnerabilities. In some countries such as the United States of America (USA), active information security programs between individuals, companies and government have been implemented (Butler & Lachow, 2012). Unfortunately up to now, no simple solution to resolve the current situation has been found simply from a government side. Governments also have to deal with increasing privacy legislation and budget constraints forcing them to follow strict guidelines and rules that are not only expensive but also extremely time consuming. The unfortunate reality is that often the cost of a security solution is then deemed too prohibitory expensive (Barclay, 2014).

Privacy demands directly hamper the ability of government to effectively monitor and police cyberspace as explained previously. Numerous examples of this limitation exist when literature is reviewed regarding national projects to combat botnet infections

(Plohmann, Gerhards-Padilla & Leder, 2011). Despite the limitations, governments cannot simply ignore the growing cyber security concerns. The need for a low cost, pro-active, easy to use, automated system is thus not only a requirement but should in fact be made a priority.

1.2 Research Objectives

This research was conducted with the following key objectives in mind:

1. To examine the potential open and commercial data sources could provide in aid of fulfilling national cyber security policy situational awareness goals. Achieving cyber security situational awareness is already a complex endeavor at organizational level, in order to determine the operational requirements for national pro-active security, it is necessary to determine the main requirements and key implementation limitations.
2. To assess available data sources in order to develop an effective pro-active security visualization tool functioning on a national level. A range of data sources are available that provide rich sources of information regarding various elements in a nation's infrastructure. By combining a selection of the datasets through data fusion, it is theoretically possible to create a system with the potential to present an overview of the national attack surface on all levels.
3. The final objective of this study was to extend the constructed system to enable automatic detection of Personally Identifiable Information (PII). This has been performed with a view to promote compliance with legislation such as the 2002 Electronic Communications and Transactions (ECT) Act (South African Government Gazette, 2003) and the more recent 2013 Protection Of Private Information (POPI) Acts (South African Government Gazette, 2013). Currently most privacy breach legislation are applied reactively resulting in expensive losses (Ponemon Institute, 2013). By automating the detection of potential privacy breaches on a national level, significant benefits can be obtained by reducing costs due to losses.

1.3 Research Method

Achieving the stated research objectives requires that a combination of research methods be applied in the study. Initially a thorough literature review has been conducted to establish a familiarity with relevant prior work. The literature study also serves to introduce the reader to previous work conducted in the field. Concepts such as

national responsibility, Internet domain demarcation and pro-active information security has been discussed in relation to information fusion and visualization.

Following the literature study, the experimental work is discussed by means of the embedded case studies approach. The choice to make use of embedded case studies were primarily due to two factors: the varying nature of the data obtained and the fact that each minor case study in this research contributes to the larger case study (Scholz & Tietje, 2002). The embedded case studies presented here focus on infrastructure, personally identifiable information and to end with the combination of the data sources. Finally, a critical analysis presents the results of the experimental system data analysis for the documented period of time in the South African domain.

1.4 Scope and limitations

The experimental work is primarily focused on assessing the viability of fusing third party data sources in an experimental system to gain awareness of the national cyber security situation. A large number of public and commercial data sources has been evaluated for this study, but not all of the sources will be implemented in the experimental system. The reasons for not making use of all datasets are examined and documented during the data source evaluation in Chapter 4. Criteria that affects the viability of the data source to be used in the experimental system are also discussed in this context. Factors such as accuracy, cost and data availability are but a few of the limitations that has to be considered. While verification of data sources is an important undertaking, the large number of data sources and data types makes this an unfeasible undertaking for this study. Instead the study has, where applicable, referred to literature as much as possible to highlight the limitation of the selected datasets.

1.5 Document and source conventions

Where appropriate, URLs for sites, software or technologies referenced in the document were listed as footnotes. The rationale behind this is to allow the reader to access the information without interrupting the flow of the narrative. In the electronic version of this document these URLs will be clickable to move to the correct section of the document. Any image or table without reference is work performed during the course of this study.

Where appropriate, code snippets has been placed as images to preserve the structure of the code with the aim of increasing readability. In instances where the information

resource is too big to be presented neatly in the document, it was placed in a folder in the accompanying DVD. Where applicable in the document, a clear reference to the resource has been provided. Details of the electronic resources provided are available in Appendix C.

1.6 Document Structure

This document consist of three parts, each consisting of multiple chapters. The research objectives described in Section 1.2 is not bound to a specific part but spans multiple chapters that can overlap parts. Figure 1-1 presents the grouping between the different parts, objectives and chapters that this document consist of. Further discussion regarding the structure will be provided from Section 1.6.1 onwards.

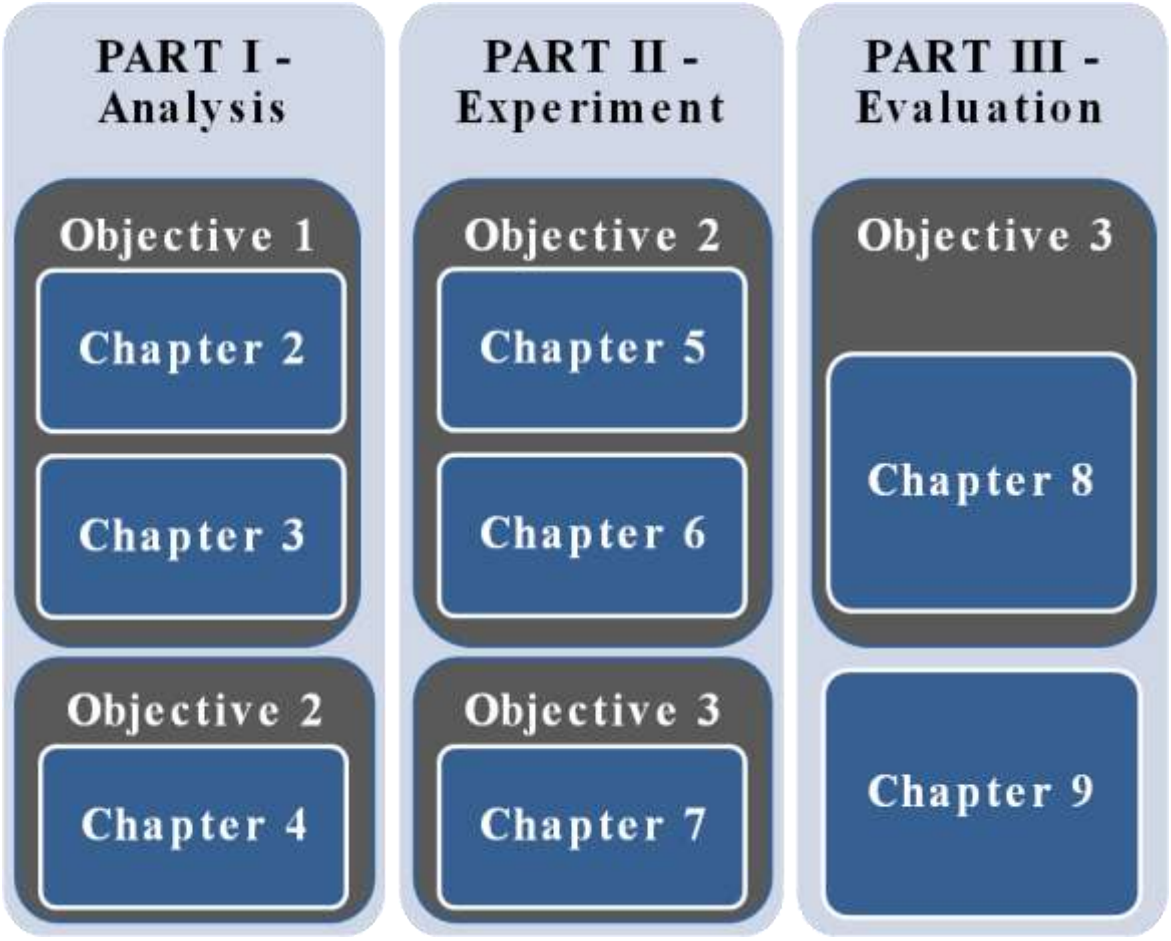

Figure 1-1: Document layout and mapping

1.6.1 PART I - ANALYSIS

These initial chapters provide an introduction into the current national cyber security environment as presented in academic literature. Implementation difficulties are discussed, as well as potential alternative sources of security information.

- **Chapter 2** – Focuses on literature related to national cyber security aspects such as cyber security policy publication, desired outcomes and implementation difficulties.
- **Chapter 3** – Builds on the content of the previous chapter and discusses concepts such as attack surfaces, pro-active security and the potential use for open source information in order to address known vulnerabilities.
- **Chapter 4** – Examines a variety of data sources that could be leveraged in order to provide information relating to vulnerabilities present on a national level. Each data source is examined in detail to describe the information that could be obtained, and to list/enumerate/identify specific limitations of the data.

1.6.1 PART II - EXPERIMENT

These chapters focus on the platforms developed, the collection of data, the implemented fusion model, and the results of two temporal case studies. Formal validation of the selected data sources against a cyber sensor evaluation framework is documented and the limitations are illustrated.

- **Chapter 5** – Introduces the fusion model selected, the architectural design of the proposed system and explores its capabilities and limitations. Design decisions are discussed in the context of legality and ethical applicability.
- **Chapter 6** – Contains the results of the study relating to commercially available data sources as a potential source of information for national infrastructure. The geographic distribution of devices within the defined borders of South Africa are discussed as well as the results of the fusion process to enrich available data.
- **Chapter 7** – Presents the results of the study that examined the distribution of PII in South Africa for a selected temporal span. The data obtained was combined in the fusion process (described in chapter 5) and the results and limitations of this approach are discussed.

1.6.2 PART III - EVALUATION

The final section contains an analysis of the results obtained in previous chapters, as well as concluding remarks.

- **Chapter 8** – Critically examines and evaluates the results obtained from Chapters 6 and 7 above in order to assess the limitations and degrees of success of the experimental system. This is done to construct a conclusion regarding the usefulness of the created system for monitoring the state of security on a national level.
- **Chapter 9** – Re-examines the stated research objectives to ensure that they have been fulfilled. This chapter concludes the study and proposes possible directions for future work.

1.7 SUMMARY

The research performed in this study examines multi source cyber data fusion visualization on a national level. The study examines both potential data sources and the data obtained through the fusion process by means of an experiment. The contribution of this study has been recognized academically through publications presented at conferences available in Appendix D. The experimental system constructed also contributed operationally to security in South Africa as discussed in case studies presented in Chapter 6 and 7. The document structure of this study is discussed in Chapter 1 and the relationship between the content presented and the research objectives is available in Figure 1-1. Chapter 2 examines the need for national cyber security initiatives and documents the various implementation limitations currently experienced.

Relying on the government to protect your privacy is like asking a peeping Tom to install your window blinds.

John Perry Barlow – Co-founder of the Electronic Frontier Foundation (EFF) in July 1992

2

National cyber security, challenges and opportunities

2.1 INTRODUCTION

Looking at potential ways and means to address cyber security is a national imperative internationally (Herzog, 2011). Not only because Information Communication Technology (ICT) contributes a significant portion of Gross Domestic Product (GDP) or because of the potential volume of individuals affected, but because governments and industry have a shared responsibility to do so (von Solms & van Niekerk, 2013). While the shared responsibility falls on all entities participating in the cyber domain, governments have a key role in the creation of policy and implementation of the created policy (OECD, 2012).

To address the need for increased cyber security, at least thirty five countries internationally have produced cyber security policies for implementation at a national level (Hathaway, 2013). The published policies vary in structure, terminology and implementation details, but all describe the same need for improved security nationally. However, publication of these documents should not be regarded as an indication of adequate national security. These policies still present a surprising amount of ambiguous terminology and lack of standards. The variance in national cyber security policies has previously been researched and highlights the fact that, while there is an increased level of awareness, significant implementation challenges still await (Luiijf, Besseling & De Graaf, 2013).

This chapter examines current literature and approaches taken by a variety of countries to address cyber security on a national level. Further discussion will focus on currently implemented projects that have an effect on national level cyber security readiness.

2.2 THE NEED FOR NATIONAL ACTION

It has been predicted that in future wars, the information space will take up a bigger role than ever before (Gasper, 2008). Several examples of this type of aggression against nation states have been demonstrated since 2004, with all key indicators showing an increase in probability of more attacks to follow (Fischer, Dudding, Engel, Reynolds, Wierman, Mordeson & Clark, 2014). Reports such as the Mandiant (2013) APT1 report highlight how persistent criminal spy activity has been a reality since the early 2000s. The use of software to influence the nuclear capability development of a nation state has been demonstrated in the form of the Stuxnet attack, highlighting the potential of the cyber domain (Falliere, Murchu & Chien, 2011). Consider that even South Africa, a country with a relatively low Internet penetration, was present in both reports. In both the Stuxnet and APT1 reports, the South African cyberspace was infected even if only in isolated instances. The Stuxnet and APT1 campaigns were certainly not the only campaigns; a steady stream of similar types of operations are regularly reported on in cyber security news sources.

Notable campaigns such as Flame, Duqu and Red October have all made headlines and provide a glimpse into the level of nation-on-nation spying and crime campaigns (Larkin, 2014). The infections mentioned have since been cleaned, but they are merely the campaigns and variants that were discovered and unknown variants could still be present on these devices. There is currently no way to ascertain the level of attack a country is under from other countries for certain. Since anonymity on the Internet can still be achieved to a large degree with sufficient skill, it becomes a exciting opportunity for a variety of actors to further their cause at the expense of others (Klimburg, 2011).

Nation states have a significant interest in cyber war since it has the potential to offer several benefits over traditional warfare approaches. In the Stuxnet example, the attacking nation targeted the Siemens Supervisory Control And Data Acquisition (SCADA) system used by Iran, altering the code programmed on the centrifugal device in order to change the operating behavior (Falliere et al., 2011). While it would have been possible to either send a team in to disable the facility, or to simply bomb the facility, the subtlety of the cyber attack is significant. Even if the Iranian government had detected the infection, there was no means to identify the attacking nation. The initial release date of Stuxnet is unclear but early variants have been documented as far back as 2005 (McDonald, Murchu, Doherty & Chien, 2013). It was only seven years later in 2012, that

the American and the Israeli governments admitted that they were responsible for the attack on the Iranian Natanz enrichment facility (Falliere et al., 2011; Sanger, 2012).

2.3 Attribution

Attribution in cyber security is the act of determining the identity of an attacker and responding to the detected attack. While this sounds fairly reasonable, the act of attribution is often not easy to obtain in the cyber environment as previously highlighted in section 2.1. A variety of reasons contribute to the complexity of attribution such as the large number of potential attackers and often sophisticated skill they posses. Often artifacts remaining after an attack can provide subtle pieces of information that potentially but not definitively provide information regarding the identity of the attacker Mandiant (2013). Artifacts such as specific tools used, templates and language can all serve to point to an attacker but not specifically prove identity.

Since it is extremely hard to attain foolproof attribution when an attack on the Internet occurs unless some sort of mistake is made by the attacking side, plausible deniability is a highly sought after attribute by nation state attackers (Geer & Archer, 2012). Accusing a nation of malicious intent without adequate proof has serious weight in political circles. It can reflect poorly on the accuser and in doing so further the cause of the attacker. It would however be optimistic to consider that a country can be taken over completely without physical resistance from the victim (Feaver & Geers, 2014). Therefore, the aim of cyber warfare on a national level should rather be considered as a force multiplier instead of a final strike. For example, although Stuxnet was an effective weapon to deny the Iranian government the ability to perform adequate nuclear research, it did not allow the creators to simply take over the government. As a force multiplier however, it could have had devastating effects. Crippling communication systems would hamper troop deployment for defense and allow attackers increased preparation time over their enemy. Cyber attacks have the potential to generate significant civil disruption, as observed in the case of Estonia (Carr, 2011).

The variety of parties compromising the cyber readiness state of a nation is found on all organizational layers. Individuals, corporations and governments all control a variety of infrastructure that enables the effective operation of a country (Luiijf et al., 2013). No single entity controls all the infrastructure that enables communication to the Internet nationally. Thus, should any crime, accident or malicious attack occur on any part of a country's infrastructure and compromise operation of the Internet, a co-ordinated effort would be require to re-establish affected operations. In instances where the Internet

connectivity was severely disrupted, re-establishing Internet communication will in all probability require international co-operation. For example, after the attack on Estonia, the national Computer Emergency Response Team (CERT) required collaboration from Finnish, German, Israeli, and Slovenian nationals to restore normal network operations to the country (Herzog, 2011). If the attack was more severe and potentially required military deployment, traditional means of arriving at a solution might have been too time consuming to be sufficient. Research has suggested that concepts such as pre-delegation of authority and instructions found in military environments could be used (Feaver & Geers, 2014). This will however only be effective if clear policies, responsibilities and processes are in place.

2.4 Anonymity on the Internet

The current situation in the cyber security environment is unfortunately far from clearly defined. Examining something as fundamental as apprehending criminals once a crime is reported, illustrates the complexity involved in the current Internet infrastructure setup. Currently, apprehending cyber criminals is hard to do due to the Praestigiae Cone layers of anonymity as introduced by Rohret and Kraft (2011). The Praestigiae layers are depicted in Figure 2-1 and this model illustrates the variety of layers available to a cyber criminal to avoid detection.

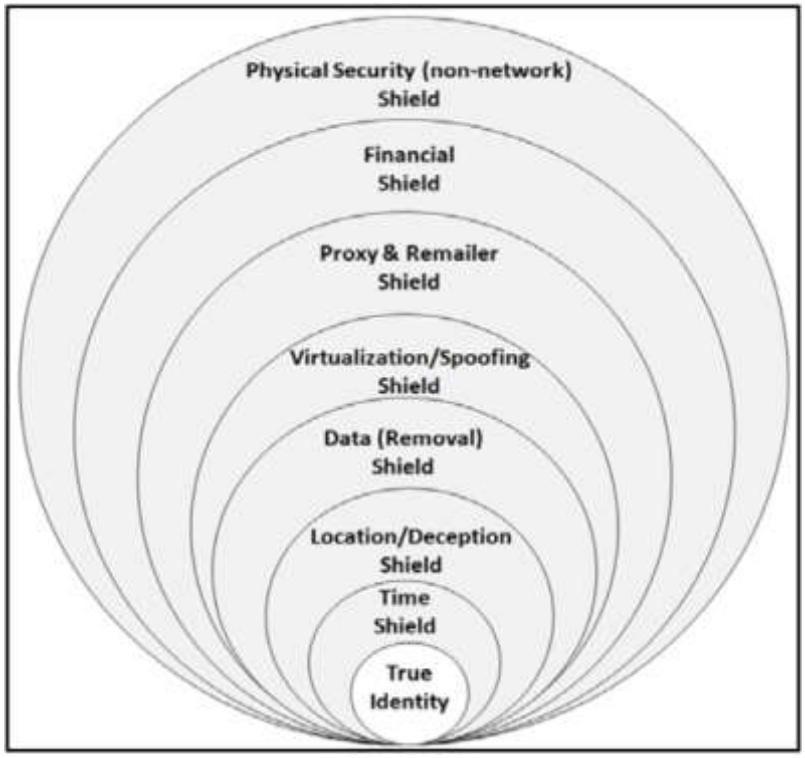

Figure 2-1: Praestigiae Cone of anonymity by Rohret and Kraft (2011)

Each layer has the potential to provide information regarding the identity of the criminal. However, the levels of abstraction and potential ease of distributing an attack over a wide variety of geographically dispersed infrastructure, makes investigation a complicated process. Collaboration between countries and entities are often required to accurately and effectively obtain information to apprehend criminals. Currently these collaborative processes are time consuming and often hamper rather than enable effective investigative work from authorities (Broadhurst, 2006; Plohmann et al., 2011). As such the majority of cyber crime investigations arrive at a dead end, finding either a previously hacked computer now abandoned or nothing at all (Feaver & Geers, 2014). In a review of published cyber security strategies, at least seventeen nations clearly identified criminals as threat actors in Intrnet security. A further five countries' strategies recognize that Internet crime does not stop at geographical borders and as such, seek to promote international collaboration (Luiijf et al., 2013).

Enough information exists to obtain a substantial idea of how the cyber underground pays. Motivations for criminal acts can be explained in the following manner. While cognizance of the illegal nature of crime is often present, the unorganized nature of the information security system often gives incentive to commit the crime (Kshetri, 2010). The current limitations of adequate information security systems and the widespread distribution of devices with vulnerabilities makes it profitable for criminals to operate on the Internet. Add to that a culture of free sharing of information and cyber crime is bound to flourish. In countries where a focus on curbing personal identity theft and controlling the flow of currency is not strong, a rise in fraudulent transactions has been recorded (Harris, Goodman & Traynor, 2013).

Achieving true anonymity on the Internet is a non-trivial exercise but with enough technical knowledge it is possible. Proposals to increase privacy on the Internet include onion routing frameworks (Reed, Syverson & Goldschlag, 1998). Onion routing aims to ensure that privacy is increased by means of encryption, anonymous relays and protocol safeguards. While several attacks on onion routing have been published in recent years, it remains one of the best methods of achieving anonymity for the general population. A popular program to achieve anonymity is The Onion Router (TOR) project[1] that was developed to increase privacy on the Internet. One of the most recent attacks against this TOR network is known as the "sniper attack" (Jansen, Tschorsch, Johnson & Scheuermann, 2014). This attack focuses on performing a denial of service attack on the

[1] https://www.torproject.org

exit relays of the TOR network and has the potential to also de-anonymise traffic if the exit relays could be controlled.

The TOR project has since its inception led to underground services available only when connected via the TOR routers, providing so called .onion addresses. Attempting to view these services while not connected to the TOR network will result in failure. This layered approach creates a significant obstacle for law enforcement investigators since there is no common log file or enforceable legal co-operation (Johnson, 2013). The TOR project is also not the only anonymising service, alternatives such as the Invisible Internet Project [2] (I2P) are also available. Even though the popularity of these implementations are increasing, TOR is at present still the most popular anonymising service in operation (Conrad & Shirazi, 2014). Alternatives to the TOR network such as I2P are growing in popularity since they provide different architectures for privacy implementation. One such example is the manner in which I2P's network infrastructure is distributed versus that of TOR. In the TOR network a centralized node of servers distribute the lists of available exit relays to potential clients. I2P on the other hand, has no central point and each relay has a list of all other relays it is able to contact. Both architecture implementations are popular and facilitate anonymous communication but both have advantages and disadvantages that should be taken into account (Conrad & Shirazi, 2014).

Examining the varying levels of abstraction available to malicious actors who wish to remain anonymous, highlights the need for both national and international collaboration. The current international environment allows individuals to subscribe to electronic services in different geographical regions to obtain access to communication or even financial services. Once a crime is reported, officials tasked with solving the crime have to start collecting information and evidence from a variety of sources. Obtaining information is a tedious, multi-step, time-consuming process that is often hampered by administrative, legal and service provider policies on a national level. As soon as international boundaries are crossed, this time consuming evidence gathering process is significantly complicated and is consequently often abandoned.

2.5 COST OF CYBER CRIME

The exact cost of cybercrime is a contentious topic with information security members stating values of between $575 Billion and $1 Trillion (Center for Strategic and

[2] https://geti2p.net/en

International Studies, 2014). Many critics of these numbers exist, such as Moore and Anderson (2011), who states than 1 Trillion dollars is 7% of the American economy's gross domestic product and more than the entire IT industry. To put it into perspective, the information security industry as a whole can still be considered a niche market due to its relatively small size. Consider that the global firewall industry, protecting critical infrastructure, was still smaller than the yogurt market of just the USA in 2012, and no individual cyber security segment is bigger than 5 Billion dollars (SANS, 2012). Since a variety of actors are affected by cyber crime, all actors' experiences will have to be taken into account for accurate measurement. This is in stark contrast with the current situation where the numbers obtained are reported by a few key players (Florêncio & Herley, 2013). A large number of organizations do not want to share incidents of cyber crime for fear of brand reputational loss, or for the potential loss of customers. Even information sharing between trusted partners regarding security incidents are not often performed due to the sensitivity of the information (Ring, 2014).

Irrespective of the true cost of cyber crime there is no denying that the loss is substantial and has been steadily growing. Consequently, measures should be put into place to secure the required investment to make ICT safer. Typically the amount to invest in securing an asset is determined by calculating the Annualized Loss Expectancy (ALE) of the asset in question (Jaquith, 2007). ALE is calculated by multiplying the Single Loss Expectancy (SLE) total with the Annualized Rate of Occurrence (ARO). The formula $ALE = SLE * ARO$ can be used as an example in the following scenario. An asset with cost R5000 that can be expected to experience a loss of R2000 once a year has an ALE value of R2000. With this in mind, it might be beneficial to the company to install a mitigation tool or process to negate the loss if a solution is available for less than R2000. Alternatively, if the loss is negligible enough, the company can simply accept that the risk exists and not implement any solutions.

Following this thinking, it should be fairly simple for companies and governments to calculate the amount that they should spend to remain secure. It is well known that the ICT sector contributes as much as 4-5% of GDP in a number of G20 countries and is set to contribute even more in future (Anderson et al., 2013). Thus, all the information is available to determine the risk amount and invest the appropriate amount to remain secure. Unfortunately much like everything in information security, all is not as it seems. ALE calculations, while very useful and popular, should be used with care and

not seen as an exact science. The current state of information security metrics is best suited for the evaluation of small components of a system (Jansen, 2010).

2.6 RESPONSIBILITY FOR NATIONAL CYBER SECURITY

Current cyber defense policies published by nations as mentioned in Section 2.1 contain lists of key national capabilities that they are striving for. Various frameworks, models and standards are being used to assess the current state and to move forward to a more secure state. One example is the guide from the National Institute of Standards and Technology (NIST) and United States of America (2014). The problem is however that once the cyber defense policies of governments are studied it becomes visible that no clear definition of what exactly will be protected is available (Luiijf et al., 2013; Cavelty, 2014), nor is scope or terminology commonly defined. Some policies contain terminology stating that the policy aims for a 'whole of government' approach to cyber security. Others have similar ideologies but rather refer to a 'whole of nation' approach (Luiijf et al., 2013).

A recent study of United States cyber defense policies have revealed that the Government is responsible for the safety of the Internet but current implementations focus on only protecting .gov and .mil websites (De Souza, 2014). This provides a clear responsibility for cyber security even if the effects do not yet reach the whole of nation. Not all governments immediately accepted responsibility for national cyber security. Australia initially made the owners of identified critical infrastructure responsible for the safeguarding of these systems. It is only in recent years that this policy has changed to make the Australian government responsible for the protection of critical infrastructure (Warren & Leitch, 2013). South Africa has legislation but responsibility for each sector of cyber security is only defined in the draft National Cyber Security Policy Framework of (2010). The final format is yet to be released and no publication data has been officially communicated. There is however a clear indication of the responsibility that the South African government has towards Internet enabled infrastructure from the draft policy. The ECT Act of 2002 (South African Government Gazette, 2003) has already set the stage for government responsibility, mandating that the .co.za domain be placed under the control of the government (Naidoo, Singh & Levine, 2013).

In instances where cyber security policies have been implemented, government has generally been identified as the responsible entity for national cyber security (OECD,

2012). From existing implementations of cyber security policies it is clear that responsibility is typically shared between different departments in collaboration with external stakeholders but that government remains responsible.

2.7 DEMARCATION OF THE NATIONAL DOMAIN

The implications of unclear definitions include unnecessary expenditure, misallocation of resources and insufficiently protected infrastructure (Ford, 2012). For example, what exactly constitutes the Internet domain of a country? Does liability stop when the IP address of the device is different from the IP address assigned to the country? Or does geographic location play an important role in the determination of responsibility? In addition, the term 'national cyber security' is often used but no generally agreed upon definition presently exists (Klimburg, 2012). This section will discuss geolocation and while a full examination of Internet routing is beyond the scope of this study, a brief introduction is provided in the next section.

The Internet Assigned Numbers Authority[3] (IANA) is responsible for the allocation of IP address pools to various Regional Internet Registry (RIR) organizations. The number of IP addresses allocated is not fixed per country but determined by the number of IP addresses the country requires. For the African continent the African Network Information Centre[4] (AFRINIC) is the RIR responsible for IP management. AFRINIC only serves the African region while different RIRs ensure operation in other areas. As an example Réseaux IP Européens Network Coordination Centre (RIPE NCC) serves the areas colored yellow in Figure 2-2.

To ensure transparency, AFRINIC maintains a updated list of IP addresses assigned to the various countries it has responsibility for[5]. Despite the availability of information from all parties involved, there are still instances where making use of one source of information might not be enough. A detailed examination of geolocation and the complexities surrounding the topic is provided in Section 4.5.2.

[3] https://www.iana.org
[4] http://www.afrinic.net
[5] ftp://ftp.afrinic.net/pub/stats/afrinic/delegated-afrinic-extended-latest

Figure 2-2: Regional Internet Registries area allocation[6]

Geographical boundaries have been presented as a means of defining Internet domain (Goldsmith & Wu, 2006). This method seems to be commonly accepted due to its economic driven incentives such as tax collection and other commercial interests such as mobile network routing (Xiang, Wang & Zhou, 2012). Attempts to establish an Internet provider that ignores borders by establishing services in international areas such as the middle of the ocean (Ford, 2012) have failed to attract significant investment, indicating that there is no significant economic incentive to have such a service. Making use of geolocation is becoming the norm and has been applied to a variety of fields ranging from taxation to content filtering by national service providers, as in France and Germany (Breindl & Kuellmer, 2013).

It would thus seem that geographical boundaries are commonly used as a means to define national interest (Demchak & Dombrowski, 2011). While this type of approach certainly holds true for the majority of national infrastructures, there are significant assets often not located in a country. Consider Table 2-1 based on research conducted by van Rooyen (2014). The research presented an analysis of the .co.za web domain hosting locations for open source content management platforms such as Wordpress, Joomla and Drupal. While the majority of the domains indexed were hosted in South Africa, a considerable number were hosted in international territory. This situation makes the use of geographic borders as territory markers rather complex considering that the percentage of hosts internationally makes up almost 46% of the top ten sample size. Protecting just the assets located inside the geographical boundaries of a country would

[6] http://commons.wikimedia.org/wiki/File:Regional_Internet_Registries_world_map.svg

thus only protect 54% of all available assets. The remaining assets would have to rely on the protection mechanisms put in place by the hosting country.

Table 2-1: Top 10 .co.za domain hosting countries in 2013 (van Rooyen, 2014)

Rank	Country	Domains hosted	Percentage hosted
1	South Africa	427292	54.4
2	United States	164607	20.96
3	Germany	101543	12.93
4	Geo-IP indeterminate	51292	6.53
5	United Kingdom	23970	3.05
6	European Union	7716	0.98
7	Canada	2817	0.36
8	Bahamas	2217	0.28
9	Netherlands	2145	0.27
10	Ireland	1803	0.23

The top 10 hosting countries listed in Table 2-1 represents 785402 of the full 813285 domains utilized in the study performed by van Rooyen (2014). As such, the top 10 hosting countries represents 96.6% of the total sample size of the experiment. The domains hosted in the countries listed in Table 2-1 were subsequently assessed for known security vulnerabilities via Common Vulnerability and Exposures (CVE) matching, and the results are depicted in Figure 2-3. The mean average Common Vulnerability Scoring System (CVSS) score obtained in the study for all deployed web implementations, is a disconcertingly high 5.4 out of a possible 10. This potentially indicates significant risk for .co.za web content that requires remediation. It could be argued that while the website is hosted internationally, local national law should still be applied. This potentially extends the borders of responsibility of the responsible entities past geographic borders into international territory.

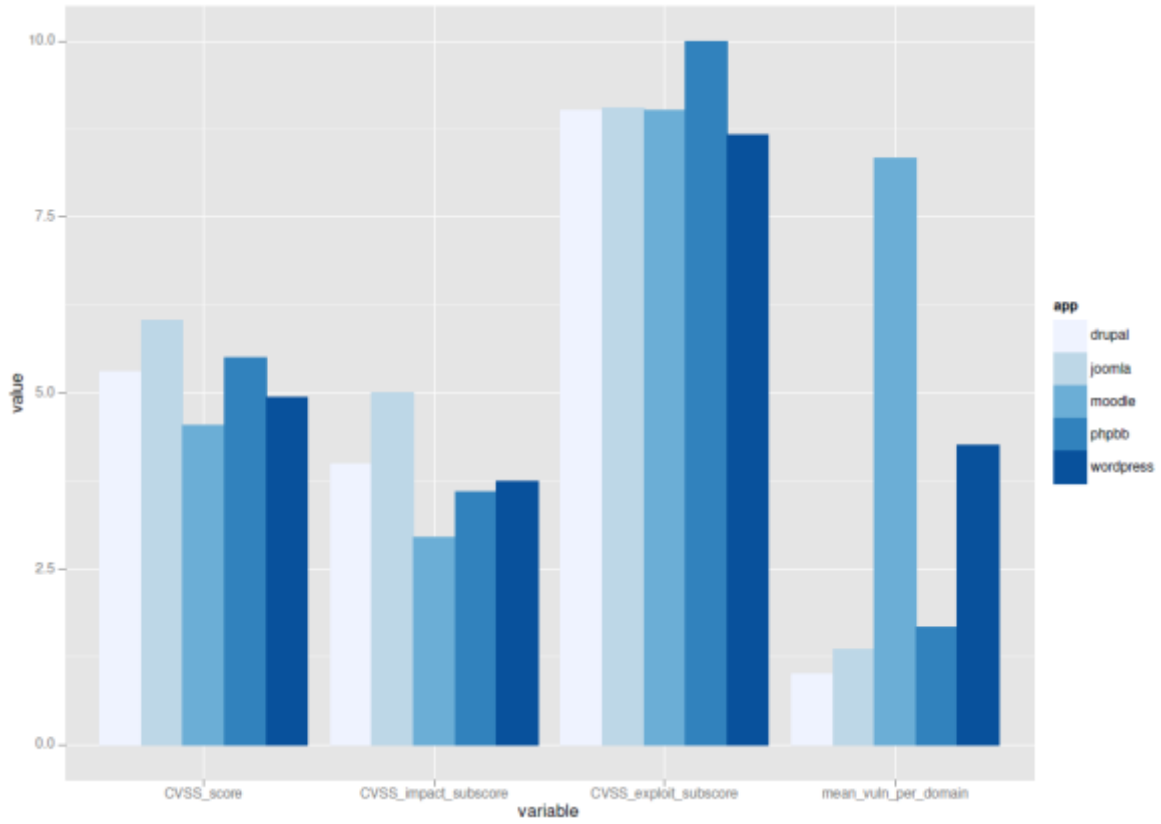

Figure 2-3: Summary .co.za hosting platform vulnerability results (van Rooyen, 2014)

In the event that a website hosted internationally was compromised and used to attack another nation's assets, a complicated scenario arises. International co-operation would have to seek assistance and information from both the hosting country controlling the web service infrastructure as well as the web service developers. Should a nation attempt to enforce some form of information security standard, enforcement of such a policy will be difficult due to international legislation. This was proven in the instance of the attack on Estonia where international Internet service provider co-operation was required and difficult to obtain (Ophardt, 2010). Consideration for events such as the complete shutdown and censorship of the Egypt and Libyan Internet is also a consideration. The shutdown proved that it was indeed possible to turn off Internet connection to a country although IPv6 traffic remained active throughout (Dainotti, Squarcella, Aben, Claffy, Chiesa, Russo & Pescapé, 2011). In the example commercial website data was used to illustrate the distribution of national infrastructure. Commercial websites are not typically seen as critical infrastructure but similar geographic distribution of recognized critical infrastructure was previously documented (Clemente, 2013).

Assuming that countries intend to make use of national borders to demarcate digital territory, the need for geolocation technical improvements will be required. In theory, IP addresses are allocated by range to a country according to the national borders but in reality this is much more complicated. Factors such as satellite connectivity and official Internet users affect accuracy of IP address allocation. These factors will be examined in more detail in Section 4.5.2.

2.8 AVAILABLE RESOURCES FOR POLICY RESEARCH, CREATION AND IMPLEMENTATION

The resources available to countries are no longer just at generic policy implementation level. Resources are emerging internationally specifically for the creation and the implementation of national cyber security strategies. A recent publication from the European Union Agency for Network and Information Security (ENISA) presents a framework to plan and implement a national cyber security policy (Falessi, Gavrila, Klejnstrup & Moulinos, 2014). The document recommends a twenty step process that follows the Plan-Do-Check Approach (PDCA) commonly found in standards such as those published by International Organization for Standardization (ISO). The initial steps are focused on defining the strategy, policy and desired outcomes which gives way to implementation when completed. Once implementation of initial desired objectives has been met, the next iteration of evaluation and re-implementation is initiated. Specific guidelines and examples are available at each steps in the process to assist policy developers with their decisions.

Current information available on national cyber security is also applicable to specialized sub policy areas as well. One such example is the *Framework for Improving Critical Infrastructure Cybersecurity* (National Institute of Standards and Technology (NIST) & United States of America, 2014). What makes this framwork unique and potentially useful is that it recognizes that critical infrastructure is not just controlled by government. The distribution of critical infrastructure can place it under the control of a range of stakeholders belonging to different commercial organizations (Clemente, 2013). These commercial stakeholders do not necessarily implement the same governing structure as the responsible department, due to different needs. The relationships between government Information Technology (IT) governance frameworks, standards and policies and those of a commercial stakeholder may vary significantly from stakeholder to stakeholder. A mapping of IT corporate governance is presented in Figure 2-4 (Jacobs, Arnab & Irwin, 2013). This serves to highlight that a range of diverse

situations could be encountered depending on how legislation requires an organization to implement the various frameworks and standards.

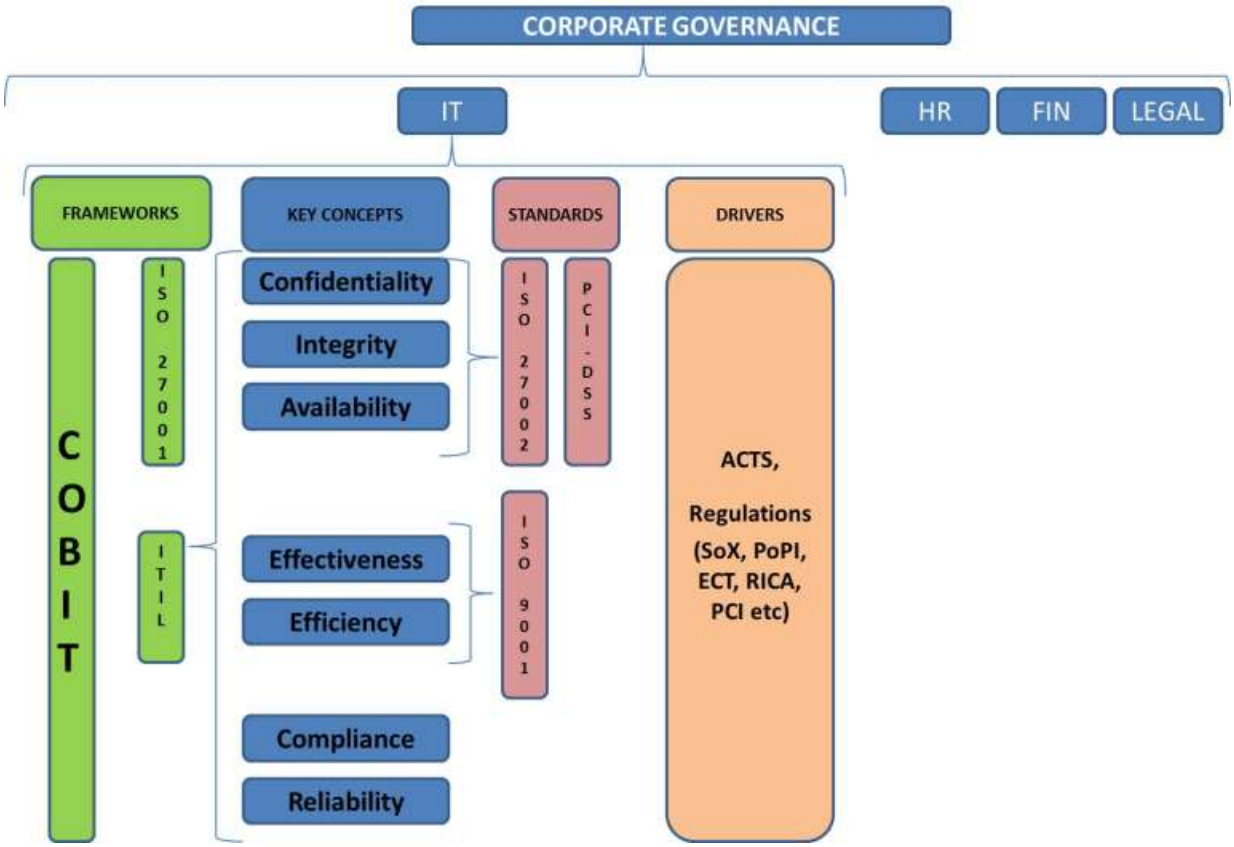

Figure 2-4: IT frameworks, standards and drivers (Jacobs et al., 2013)

This diversity increases the cost of communication, co-ordination and information sharing, and slows down implementation if not managed correctly. The NIST critical infrastructure protection document recognizes this need for co-ordination and sections of the document are mapped to common industry standards. Consider Figure 2-4, depicting the relationships between technology frameworks, standards and drivers commonly in use today. A significant number of organizations strive to have good corporate governance and implement a variety of frameworks and standards to adhere to regulations and legislation. To effectively communicate with these organizations, a large increase in co-operation can be achieved by adhering to known corporate governance techniques (PWC, 2014).

The NIST critical infrastructure protection framework aims to achieve collaboration between organizations and government on a national level. By proposing a generic five-step program within the framework, the developers retain the concept of the familiar PDCA prevalent in security standards. The five steps are:

- Identify
- Protect
- Detect
- Respond
- Recover

What makes the NIST critical infrastructure protection framework unique is the relevant mapping of the five step process to the existing corporate governance frameworks and standards in use today. Figure 2-5 shows how the Identify step is broken down into smaller achievable steps. These steps then directly map to the commonly used governance frameworks and standards. This will allow any organization with a sufficiently implemented governance strategy to collaborate on the requested information and tasks.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

Figure 2-5: NIST critical infrastructure standards mapping (National Institute of Standards and Technology (NIST) & United States of America, 2014)

Implementation of a national cyber security policy is not just about technical solutions; careful consideration should be given to the parties that need to participate and their infrastructure and business incentives. Previous research has shown that early warning

without the correct incentives will not guarantee the resolution of the disclosed security vulnerability (Cavusoglu & Raghunathan, 2007).

2.9 DOCUMENTED POLICY IMPLEMENTATION DIFFICULTIES

While policies are available and several countries have made significant progress in addressing these concerns, an abundance of implementation challenges remain. This is to be expected from an undertaking of such significance, but the difficulties identified in the following sections have significantly delayed implementation and should be considered. Failure to properly evaluate all areas of a national system can provide a false sense of optimism with catastrophic consequences should any of the components fail. This false sense of optimism, can often be the result of poor planning, but it has been proven previously that humans are ill suited at evaluating probabilities in a complex system (Shanteau & Stewart, 1992). The next subsections will address some of the documented implementation difficulties.

2.9.1 COMMON DEFINITION

Dr Peter Shergold on 15 October 2003 stated that "*A policy which is embraced by a Minister, approved by Cabinet, announced publicly, but inadequately delivered, is worse than no policy at all*". The publication of national cyber security strategies and policies is typically seen as the first step to a more secure country. There are however significant challenges that limit the effectiveness of these publications. Some of the challenges are as basic as finding an internationally accepted definition of cyberspace and cyber security or even just cyber crime (Morris, Pan, Lewis, Moorhead, Reaves, Younan et al., 2011; Luiijf et al., 2013; Lewis, 2014). Gaining a common definition is key to the mutual understanding of concepts which will allow greater co-operation with international partners. Since international co-operation is listed as a key requirement in a majority of published cyber security strategies, common definitions remains a challenge (Lewis, 2014). This limits the efforts of international crime enforcement agencies significantly, since what is defined as a crime in one country, is not necessarily a crime in another (Spring, 2013).

It is not just generalized definitions such as cyber space, cyber security or cyber crime that remain problematic. There is no international definition of critical infrastructure (Clemente, 2013). This is hardly surprising considering definitions of critical infrastructure are not constant nationally either, but evolve over time. To substantiate this claim, consider that the United States has published various classifications defining

critical infrastructure from as early as 2002 (Moteff & Parfomak, 2004). These publications mainly identify categories of critical infrastructure such as power, ICT and sanitation. These categories are constantly updated and this is necessary as new information becomes available, but it also causes disruption for the sectors affected. To be identified as a critical infrastructure sector requires a variety of policy implementations for that sector. These policy implementations have monetary value attached and it affects morale if a sector is removed after significant work has been undertaken.

The emerging field of Internet governance further complicates the matter by stating that what is defined as critical infrastructure in the real world, might not be considered critical Internet infrastructure. Instead, only infrastructure that directly impacts the Internet operation on a global level can be considered critical (DeNardis, 2010). This distinction in terminology is understandable when the Internet is considered as critical infrastructure. Unfortunately the distinction adds complexity and confusion regarding what is classified as critical infrastructure on top of existing ambiguous definitions.

For the purposes of this study, cyber security will encompass all aspects affected by and related to the digital domain. This includes the human component (von Solms & van Niekerk, 2013) as well as infrastructure such as communication networks (Bishop, 2003).

2.9.2 Implementation strategies and measurements

Also severely lacking in the published national strategies are implementation strategies and measurements. The national cyber security policies address the topic of what is required to have a good cyber security posture, but in most instances fail to specify how this vision will be achieved. Implementation of the published strategies are vague at best with very few clearly defined targets or implementation dates and goals. Only a select few of the policies published implement any form of the recommended Specific, Measurable, Achievable, Realistic and Timely goals (SMART) (Luiijf et al., 2013). Implementation goals are critical to the success of cyber security policies and the lack thereof can lead to ineffective enforcement (OECD, 2012).

Countries such as the USA that have significant investment in national cyber security programs, still have their share of failures. A recent report by the US Homeland Security department details a significant number of cyber security incidents that affected both governmental and military networks. Examples of failures stretch from the

mundane weak passwords, to the critical theft of a nuclear plant's cyber security protection plans (Coburn, 2014). These failures were not by private organizations doing business with the government, but by the federal government bodies themselves. The lack of implementation goals might be purely due to the large scope of the projects but even that should have been a consideration in the beginning of policy creation.

A significant body of research and projects have attempted to address unsuccessful implementation of cyber security. Considerable international resources have been made available by various security organizations to assist with policy implementation both in a generic and specific manner. For example, the Australian government has published a generic framework to ensure that policies are drafted in a way that supports implementation (Falessi et al., 2014).

2.9.3 INEFFECTIVE LEGAL ENFORCEMENT AND EXCESSIVE LEGISLATION

While policy and legislation might state that a certain action is illegal, the law is often only as strong as enforcement. Police forces are typically seen as the responsible entities for enforcing government implemented legislation, but as illustrated by Bossler and Holt (2012), police officers do not necessarily feel the same way. The situation in South Africa is typical of other countries where the traditional methods of the police are simply not adequate to enforce cyber legislation (OECD, 2012). This inability to enforce legislation is not necessarily due to a lack of commitment organizations such as the South African Police Service (SAPS). Rather the lack of enforcement can be attributed to the lackluster pace of change in a organizations the size of SAPS and a critical lack of skills, tools and trained personnel (Kyobe, Matengu, Walter & Shongwe, 2012).

South Korea in 2012 abandoned legislation that required all individuals to navigate the Internet using no aliases but their real names. The original reason for the legislation stemmed from policy that aimed to reduce Internet crime and dissent. The final reasons cited for the abolition of this legislation were privacy concerns but also the difficulty in enforcing such legislation (Feaver & Geers, 2014). South Africa has its own legislation, the ECT Act, which states in Section 5 that any and all cryptographic providers must be registered with the Department of Communication (South African Government Gazette, 2003)[7]. Yet, new cryptographic products are freely downloaded from a variety of application stores, the Internet and even custom developed for individual organizational

[7] Now the Department of Telecommunication and Postal Services

need without any such registration. To date, no public announcement of the enforcement of this legislation has been made available.

If the only problem was that the legislation is not effectively enforceable, it could be considered an oversight. Unfortunately, as a byproduct of stringent regulation, information security research is not contributing to national security as it could (Doherty & Hawkey, 2013; Bankston, Ford & Hofmann, 2014). What this ineffective and excessive legislation currently achieves is simply to discourage researchers from providing valuable information to authorities for fear of prosecution. There has been a steady increase in the number of security researchers sentenced under computer crime law internationally that discourages security research (McGuire & Dowling, 2013). Even reporters such as Barret Brown that strived to report on the current situation of information security have been prosecuted for merely disseminating already public information (Norton, 2015). The perceived excessive punishment has created the impression that it is dangerous to actively inform the public regarding existing threats thereby deterring community engagement.

2.9.4 STAKEHOLDER ENGAGEMENT AND INFORMATION SHARING

National cyber security implementation requires action from all stakeholders connected to or delivering a service. With the large number of stakeholders involved, implementation difficulties such as unwilling public participation, internal politics, privacy concerns, cost and loss of reputation fears have all been documented (Dlamini, Taute & Radebe, 2011; Klimburg, 2012). An example of the types of concerns raised is found in the USA critical infrastructure protection plan. The Einstein 3 application has been proposed by the USA government for implementation between all stakeholders, but not everyone agrees that it is the best course of action. Factors such as the difference in scale between the federal government and private industry, the inability to specify hardware and the difference in governing frameworks were mentioned (Bellovin, Bradner, Diffie & Landau, 2011). These are legitimate concerns raised by researchers and organizations and should be communicated well before a tool is selected for implementation. Critical infrastructure might have been under the sole control of governments in the past but privatization and government divestment is rapidly placing the control with individuals and organizations (De Bruijne & Van Eeten, 2007).

Providing the correct incentive to secure a system is considered as functionally important as providing a secure architecture for a system (Anderson & Moore, 2006).

The entity responsible for the system's security is often not directly affected by the failure or compromise of the system. This simple misalignment of incentive has been documented extensively as one of the key drivers why new practical information security technology does not get deployed. Recent research even suggests that the emerging field of selling cyber insurance might negatively affect the overall state of information security by de-incentivizing responsible parties (Pal, Golubchik, Psounis & Hui, 2014). Ample research is available to improve the security posture of a nation should all stakeholders choose to participate. As an example, research detecting the use of fast flux Domain Name System (DNS), typically used in malicious botnets, is already available (Stalmans & Irwin, 2011). Unfortunately Internet Service Providers (ISP) rarely implement such technology since it would require additional investment with hardly any additional financial benefit to them (Hofmeyr, Moore, Forrest, Edwards & Stelle, 2013). It is not feasible for another entity to implement the technology since ISPs are the only organization in possession of the network traffic and affected client details (Geer, 2010).

2.9.5 PRIVACY CONCERNS

The number of times that data from citizens were requested from social media organizations such as Google, Facebook, Twitter has recently increased from nation states (Dalal, 2014). The increased surveillance and information requests have sparked an outcry over the potential loss of privacy in the name of national security. The fear that privacy will be lost in a surveillance state has even spurned researchers to find methods to combat mass surveillance. Shay, Conti, & Hartzog (2013) presents a taxonomy of possible methods to combat mass surveillance in the modern age.

The removal of malware from users' computers is another interesting aspect to consider. Gaining access to the infected computer can potentially be achieved once the malware is reverse engineered, but this type of access is illegal in nearly every country. This creates a situation where the solution is available to the authorities to clean the malware infected machines, but to do so would be considered illegal. Should any of the machines fail during the clean up process, the authorities would be potentially liable (Plohmann et al., 2011).

While the privacy aspect is mainly related to the public perception of excessive monitoring, sharing between organizations are not happening effectively either. Security information by its very nature is deemed sensitive and this limits organizations affected by cyber incidents to effectively share information (T. Moore & Anderson, 2011).

2.10 Inability to act on vulnerable inventory items or achieve inventory

A variety of information security vulnerabilities can affect the operation of a country. Open resolvers (discussed in more detail in Section 4.5.9) is one such example. Incorrectly configured DNS infrastructure, widely available in any country, can be used to cripple communications. The threat is not trivial and a comprehensive database has been compiled as a result by the Open Resolver Project[8]. The database is maintained and is used to track the decline of this vulnerability over time. Considering that the root problem is simply an incorrectly configured DNS service on a device and that all the information is available to authorized national entities, it is surprising that only a slight decline has been achieved. This inefficient national clean-up highlights the need for stronger collaboration with partners such as ISPs, who would be able to provide contact details for the affected devices.

While the presence of open resolvers is a threat to the smooth operation of a country, it has not received nearly the attention that critical infrastructure aspects have. The need to inventory and comprehensively protect critical infrastructure is mentioned in nearly every national cyber security policy (OECD, 2012). The process for critical infrastructure detection however, is far from trivial. Identifying critical infrastructure typically involves the compilation of assets that need to protected as part of a formalized process. The USA critical infrastructure protection plan (Homeland Security, 2014) is depicted in Figure 2-6. The process of selecting critical infrastructure is typically a manual process and current implementations are often performed in a distributed manner. This results in inaccurate details being captured since depending on the stakeholder, the definition of a critical resource will vary. Consider that the US Department of Homeland Security National Asset Database contained over 77000 items in 2006. Some of the assets listed in this report were petting zoos and car dealerships (Clemente, 2013).

[8] http://openresolverproject.org

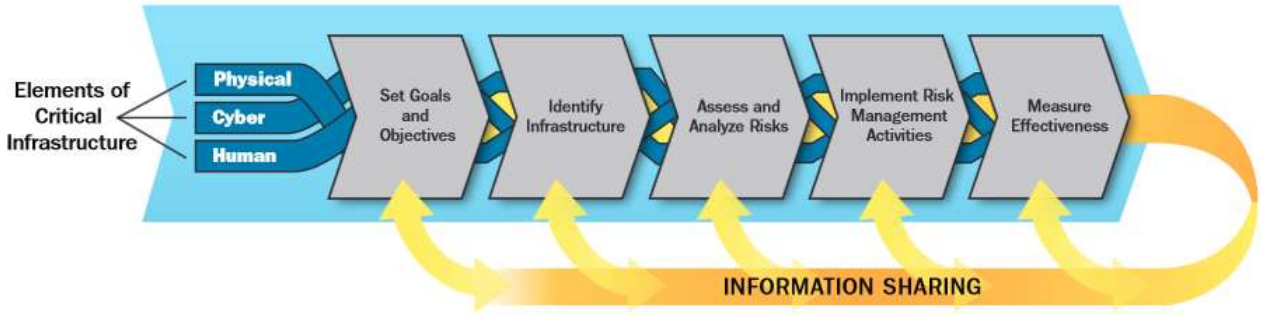

Figure 2-6: USA critical infrastructure protection plan (Homeland Security, 2014)

The ability to automate the detection of critical infrastructure is currently not a reality. Simply placing a specialized scanning tool on the network to search for specific device or protocol signatures could have disastrous effects. By way of example, the mere act of scanning a SCADA device could cause it to malfunction (Permann & Rohde, 2005). This limitation has generated significant research and even delivered commercial systems such as Cyberlens[9]. The effectiveness of the research and proposed systems remains untested however. Should a government or private entity start performing scans, they could potentially incur liability for any scanned devices that consequently malfunction.

Even if it was possible to scan for critical infrastructure in a manner that negates this risk, assessing the actual security state of a device is hard to achieve. Measuring security posture can be achieved by two methods, either auditing or assessing (G. Williams, 2012). Auditing is a process of checking to see that the subject under evaluation conforms to previously defined criteria. Assessing on the other hand is a more active and intrusive process. While auditing can achieve a good standard of adherence by following an approved international standard, assessment relies heavily on the skill and testing methodology of the individual or team responsible. Vulnerability assessment looks for vulnerabilities in the system while a Penetration test (pentest) confirms that the vulnerabilities are exploitable. It should however be noted that while a pentest is a relatively good indicator to assess if a vulnerability is exploitable, there is an increase in risk to the system under assessment. Should the pentest be performed in such as way that the risk is minimized, more limitations have to be considered. Factors that influence the reliability of the pentest, such as operator skill, limitations placed on the operator and amount of time provided, all limit the usefulness of manual labor on a national scale.

[9] http://dragossecurity.com/products/cyberlens

Thus, to achieve large scale security evaluation, automation will be a key factor. The requirement has long existed in commercial operations and several automated tools have evolved into sophisticated platforms for assessment and penetration testing teams. These tools typically contain libraries of available exploits and in many instances have the means to automatically exploit given vulnerabilities on systems. Several considerations need to be taken into account when deploying this technology, as vulnerability scanners are not perfect and often can be fooled by seemingly insignificant variables in the target environment. The applications are often prone to false positives (Doupé, Cova & Vigna, 2010); each false positive needs to be investigated and confirmed that it is indeed a mistake on the scanning software's side.

Further research shows that even state of the art vulnerability scanners can have trouble determining if the Windows machines are correctly patched (Badawy, El-Fishawy & Elshakankiry, 2013). Further research has shown that setting the language of the system to something other than English can severely degrade vulnerability detection (Holm, Sommestad, Almroth & Persson, 2011). Once the language is set back to English and the test re-run without changes to the system, a higher percentage of vulnerabilities were detected. This type of inconsistency was not uniform to all vendors, highlighting a further problem in the use of vulnerability scanners. At this point there is no uniform standard for detecting vulnerabilities. If a vulnerability assessment is conducted with three different vulnerability scanners, the probability that three different results will be obtained are high, necessitating further human intervention.

The emergence of active defenses for network devices makes matters more complicated. Active defenses increase the uncertainty that the device detected is indeed the correctly identified device. This is done to create misinformation regarding the devices located on the network since vulnerabilities very rarely affect all computing platforms equally. Typically successful exploitation requires a specific device or software version to be successful. Thus, while the active defense system will fool attackers, it will also create even more uncertainty for an attempted inventory implementation.

2.11 SUMMARY

The need for national cyber security is evident, despite the array of factors limiting information security stakeholders tasked with its implementation. A summary overview of key limitations were discussed in extra detail but it should be noted that additional complications exist. The limitations identified are not trivial to resolve and make the

prospect of achieving satisfactory cyber security on a national level seem improbable in the near future. While resources to assist with policy creation, implementation and evaluation are emerging, establishing political will and gaining co-operation from all role-players will remain a time consuming process. There is thus a unambiguous need to improve national cyber security in a expedited manner with the resources already at hand.

Chapter 2 established the need for national cyber security policy publication and implementation. The chapter highlighted current implementation challenges that will be hard to resolve in the near future. Chapter 3 takes cognizance of the fact that implementation difficulties exist but proposes that there is a significant potential to increase collaboration through open source data fusion and visualization. Should more effective collaboration occur, it has the potential to increase the cost for attackers by denying them the ability to use free information. To illustrate this, Chapter 3 will address topics such as attack surfaces, economics of cyber attacks and the potential to use open source information on a national level. These topics are discussed to underscore how effective use of open source information could potentially increase collaboration and raise the cost for attackers seeking to attack national assets. In turn, these actions will contribute to achieve the objectives set out in national cyber security policies.

In theory, one can build provably secure systems. In theory, theory can be applied to practice but in practice, it can't.

M. Dacier – Sr. Director: Symantec Research Labs

3

National cyber security situational awareness

3.1 INTRODUCTION

Chapter 2 described the need for action to be taken at a national level to address cyber security. A cursory examination of the published national cyber security policies were presented together with their respective implementation limitations. Lack of progress on policy development and implementation were attributed to a wide range of factors including: cost, limited information sharing, privacy concerns, excessive legislation and lack of cyber security experts. Information sharing was highlighted as the key requirement since it is central to a large number of related concerns. The request to share information security event information is not however, a new requirement. Various international governments have created departments to facilitate sharing of information and provided resources to assist in the event of a serious incident. Despite these efforts, only a limited number of implemented programs have achieved significant participation interest. While the sharing of information does have the potential to improve the information security posture of the collaborators, it does not necessarily safeguard a whole nation's infrastructure.

This chapter builds on the information provided in Section 2.7 by providing a brief summary of the attack surface of a nation in Section 3.2. A brief examination of information sharing requirements from various organizations and actors are then discussed in Section 3.3. The advantages and disadvantages of pro-active vs. reactive security is briefly discussed in Section 3.4 to highlight the difference in approaches. Finally a discussion on the potential open source datasets have to provide information regarding the security readiness of a nation is presented in Section 3.6.

3.2 DEFINING THE ATTACK SURFACE

A threat can be defined as any situation where a capability, an opportunity and sufficient intent to harm is present (Gasper, 2008). Considering the previous statement, it becomes clear that of the three variables required for a threat to exist, only one is in the control of the defender. A defender cannot control the capability the attacker has, nor can a defender control the intent the attacker possesses. Thus, the only variable that the defender can attempt to negate, is the opportunity to exploit. To achieve this, a clear understanding of the potential opportunities or 'attack surface' available to an attacker is required.

The attack surface of an entity can be defined as the "*exposure area that remains reachable and vulnerable to attack*" (G. Williams, 2012). Calculating the attack surface of an entity can be achieved by examining the three key components of any system (Carr, 2011):

- Hardware
- Software
- People

Having only three components to examine should by no means lull researchers into a false sense of security. The three components categorize a vast number of smaller entities. All of the entities and their various interactions need to be taken into account when considering the attack surface of a company, product, organization or nation. The complex interaction between the various systems presents an attacker's advantage, defenders dilemma situation (LeBlanc & Howard, 2002). This refers to the fact that an attacker has to only find one flaw that allows access to a system as shown in Figure 3-1. In contrast, a defender has to protect and monitor a large number of assets and complicated system interactions to defend the system. In Figure 3-1, the line depicted in red is the attack path that succeeded for the attacker.

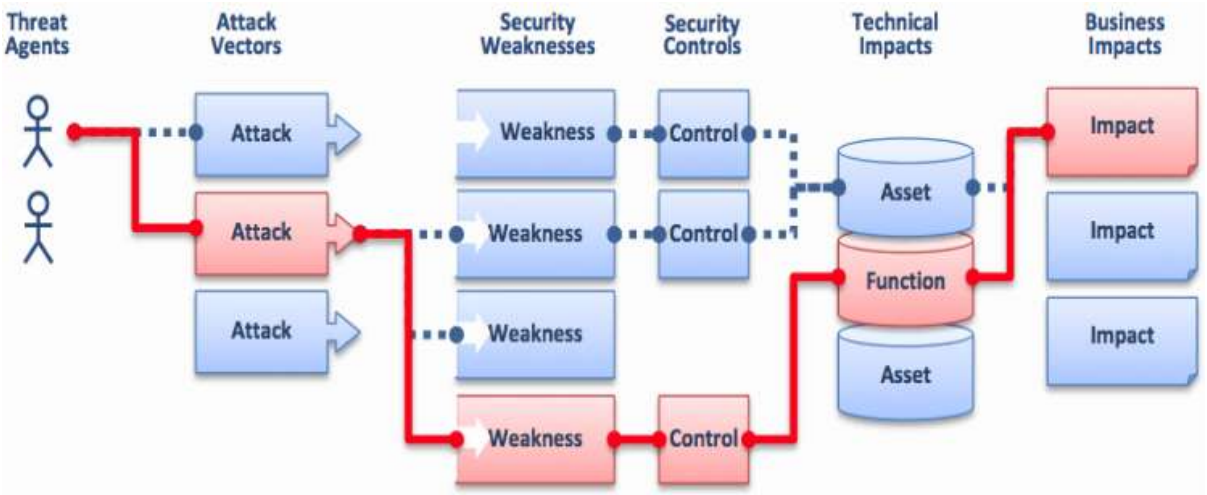

Figure 3-1: Attackers advantage, defender dilemma (Kachhadiya & Benoist, 2012)

As a simple example, consider an attack on a commonly found Radio Frequency Identification (RFID) protected door lock. All three of the components previously discussed and depicted in Figure 3-2 play an important part in ensuring authorized access. Basic rules for the example system are as follow:

- The *hardware* component upon receiving a signal from software ensures that the door is opened, and afterwards closed
- *Software* reads access cards and determines if the card is authenticated when presented
- Uniquely coded access cards are only provided to authorized *personnel*

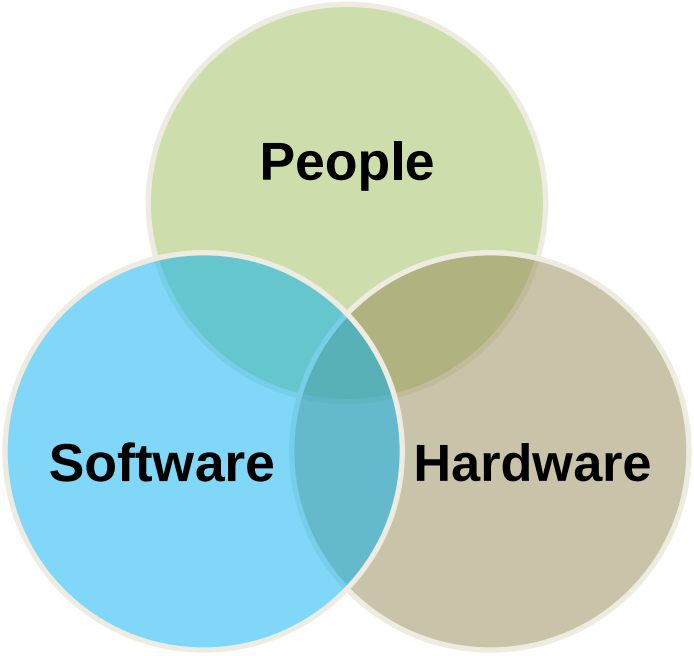

Figure 3-2: Basic attack surface of a security system (Carr, 2011)

The system described above only functions according to specification if all entities in the system participate correctly. A breakdown in any of the components causes a breakdown in the confidentiality, integrity and availability of the system. In the following section known attacks on electronic door locks are discussed as illustration of the concept.

3.2.1 HARDWARE

Babak and Deviant at DEEPSEC[10] (2012) illustrated a variety of attacks such as making use of an extremely strong magnet to move components inside the lock to the required positions. For example, the Devil Ring magnet attack involves placing a round magnet on the door handle and spinning it either clockwise or anti-clockwise to open and close the lock. Another attack illustrated was performed by simply jamming a paperclip wire into drainage holes at the bottom of the lock to reach the internals of the lock and force it open.

3.2.2 SOFTWARE

Since most electronics require at least some sort of software program flow to allow the electronics to perform the intended function, software contributes to the attack surface of the device or system in question. An incident was reported where Google's Australian offices located at Wharf 7 were attacked (Kim, 2013). The device in question was a building management system that controlled security and environmental controls. The attack involved obtaining the firmware present on the device which was possible since manufacturers typically require devices to be upgradable over the Internet. Once the firmware was extracted, it was reverse-engineered and found to contain a master password inside the firmware that allowed the attackers full control over the system.

In another incident, Cody (2012) demonstrated how commercially deployed electronic door locks used in hotels are vulnerable to attack. The researcher found that while the lock seems physically secure, the device software allows all memory in the device to be read with no authentication. With the use of an Arduino to access the memory, the researcher was able to obtain the master keys located in the door lock and open any device with the vulnerability in rapid fashion.

[10] https://deepsec.net

3.2.3 PEOPLE

An attacker can attack the people component by either cloning or stealing the token from an authorized personnel member, currently from as far as 92cm (Fran, 2013). While theft is always difficult to guard against, the arguable bigger risk is that the authorized card will be cloned. While theft is a real risk, the time frame for discovery is typically significantly shorter than that of cloning. RFID was designed to have a relatively short range of operation to ensure proximity, but several notable attacks have been observed. The RFID attack taxonomy performed by Mirowski, Hartnett and Williams (2009) depicted in Figure 3-3 will be used to further examine this component of the attack surface.

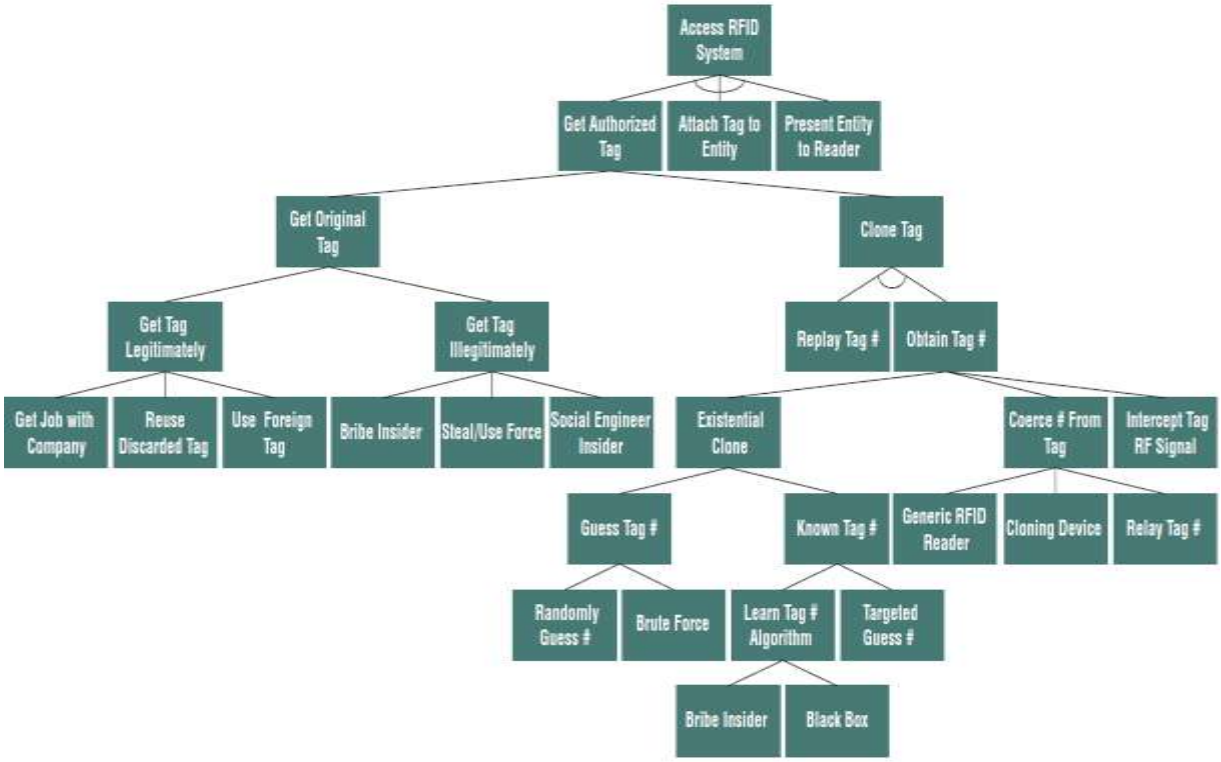

Figure 3-3: RFID attack taxonomy (Mirowski, Hartnett & Williams, 2009)

The information contained in Figure 3-3 starts off with the RFID system at the top. It immediately identifies that in order to access the resource protected by the RFID security system, the entity in control of the RFID tag could simply be presented to the system for authentication. Further attacks include examples such as social engineering a insider or bribing them for the authenticate card. Through the number of potential attacks available, the taxonomy presented in Figure 3-3 illustrates just how important it is to include the human aspect in attack surface calculations.

3.3 INFORMATION SHARING

The RFID example provided in the previous section is merely an illustration of concept. To adequately examine the attack surface of a country is a non-trivial undertaking. Regardless of the enormity of the task, the fact remains that information sharing should be a priority if any success wishes to be achieved nationally (Barnum, 2013; Falessi et al., 2014). The need for information sharing is grounded in the fact that no single entity controls all of the infrastructure connected to the internet as discussed in Chapter 2.6. In order to obtain comprehensive situational awareness, information sharing is the only option for interested parties (Kornmaier & Jaouën, 2014).

Determining what to share is unfortunately not a trivial task. Consider the previous sections that used a simplistic example to illustrate the attack surface of an electronic door lock. Now consider that nearly every system connected to the Internet has a similar attack surface to a varying degree. Figure 3-2 presents the basic principles required to examine the attack surface of a system but the reality is far more complex. In an effort to increase the measurability of security, the MITRE[11] corporation has significantly extended the work on attack surfaces[12]. The extended attack surface categories represent a more realistic categorization of the attack surface points of an organization. These extensions allow for increased information sharing through various available protocols at specific layers. This will in future serve to decrease the entry barrier for information sharing as the NIST policy to standards mapping (Figure 2-5) attempts to do for critical infrastructure information sharing.

Current efforts to achieve security are complicated by the complexity of the cyber environment. Table 3-1 gives summary of the most prominent complexity factors. The factors mentioned point to either a lack of relevant information or a lack of ability to effectively process the information.

[11] http://measurablesecurity.mitre.org
[12] The extended categories presented by MITRE are available in Appendix B

Table 3-1: Cyber information sharing complexity (Giacobe, 2013)

Complexity	Description
Security as a collateral study	Small organizations add network security as additional duties to network or systems administrators
Division of Labor	Large organizations divide roles of security, which put up information sharing walls between defenders
Lack of Physical domain	There is no limitation of time and distance. Hackers can penetrate systems from around the world and a all hours of the day
Reliance on sensors	There is no way to directly observe the cyber environment. It must be observed by sensors
Rapidly evolving attack vectors	New attack vectors emerge frequently
Automated attack tools	Hackers do not need to be sophisticated, they can use existing toolkits to launch attacks
Confusing defensive tools	Defensive tools are difficult to use and have a high learning curve
Lack of integration of defensive tools	Defensive tools exist in their own silos and do not share information between each other
High false alert rates	In particular, IDS systems are notoriously high in false alarm rates
Lack of future projection	Systems have no ability to project a hacker's next likely step

The difficulties listed in Table 3-1 are all valid concerns of the current defenders' situation. It does however not reflect the reality that attackers are also dependant on information for attacks to succeed. Whilst Hutchins, Cloppert and Amin (2011) examined the attack patterns of adversaries they noted: "*It is possible to anticipate and mitigate future intrusions based on knowledge of the threat*". Effective information sharing can deny attackers the ability to reuse the automated tools they created for attacking a company. When defenders have the ability to share information effectively, future attacks can be prevented by forcing the attacker to find a new avenue of attack. An illustration of this type of behavior is presented by Bianco (2013) as the pyramid of pain in terms of cyber attacks in Figure 3-4.

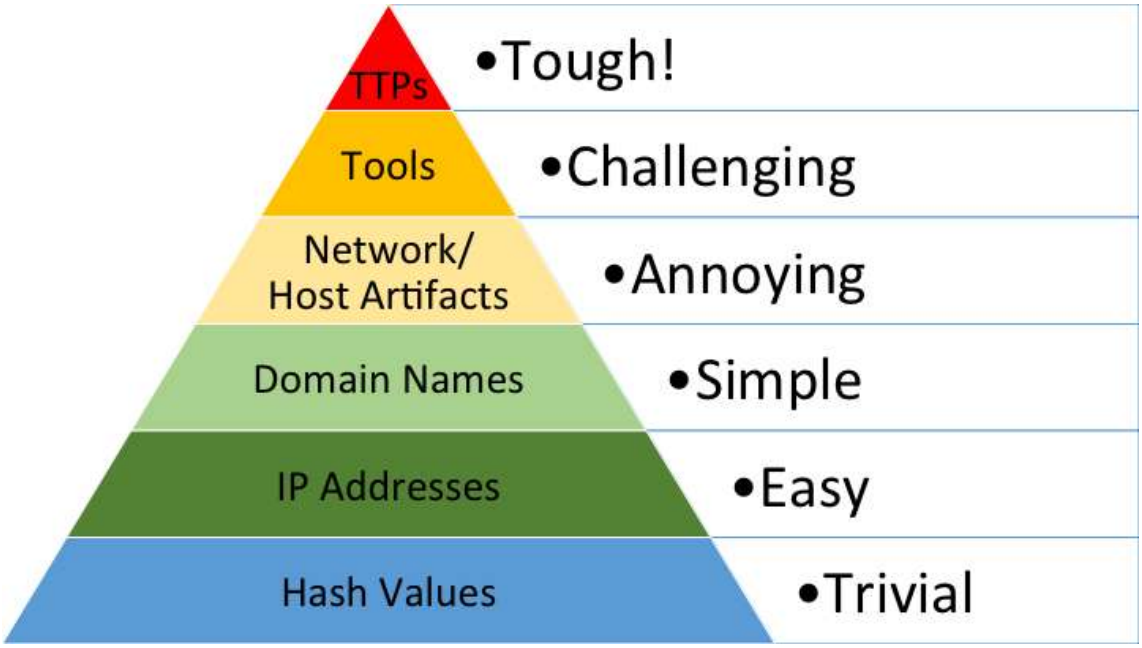

Figure 3-4: Pyramid of pain as related to cyber attacks (Bianco, 2013)

The pyramid of pain depicts the difficulty inflicted on the attacker, should the defender have the ability to negate the attacker's information flow. At the bottom of the pyramid are hash values that can be generated if any of the attacker's infection modules are detected. While this will stop the attacker from re-using the specific executable that was flagged as malicious, it is trivial to alter the hash value and thus avoid detection (Swart, 2012). The next layer 'up' refers to the IP address that the attacker uses during the course of the attack. Spoofing an IP address is fairly simple to do and should not present too much of a stumbling block for the attacker. The domain name layer is next and with the ability to register domain names in bulk, it does not deter the attacker too much. At the very least it forces the attacker to expend more money with the registration of additional domains.

At the layer marked 'Network / Host artifacts', a defender can detect intrusions based on network communication patterns or host artifacts. While changing the hash of a tool as previously described is not complex, altering the functionality to remove the detected artifact requires significantly more work. Should the defender be able to detect the attack via the communication used by the attacker, it would force the attacker to alter the communications used between different binaries. Changing communication functionality is much harder and resource intensive, since the communication channel is typically shared between all components. Thus, to change communication, all binaries used in the attack would need to be altered.

Further up the pyramid is the section labeled tools and these are typically more specialized binaries used once access to the host is achieved. Privilege escalation, data exfiltration and persistent backdoors are all examples of binaries that could be used. Development of these tools is a time consuming process and can significantly slow down an attacker if they are forced to change to different frameworks. At the very top is Tactics, Techniques and Procedures (TTPs). This jointly describes the identified attack method and the defense tactics used in response to the attack. Should it become possible to share information regarding this, it would force the attacker to not just alter technology but also approaches to targets. This is not a trivial exercise since the attack is also a technical operation that needs to be planned.

From examples discussed in previous sections it is thus clear that sharing of information has the potential to not only benefit defenders but also can deter attackers significantly. Sharing requirements vary depending on the defenders' needs, strategies and limitations. Government department information sharing requirements are different from that of a small business owner. However, if a small business owner had access to vulnerability information related to owned infrastructure, a potential data breach could be averted. This sentiment is substantiated by Lewis, Louvieris, Abbot, Clewley and Jones (2014) in an assessment of small and medium business sharing requirements Figure 3-5. The authors add that not all information is relevant to all organizations and this fundamental difference complicates current sharing implementations. Current collaboration platforms would have to take cognizance of different sharing requirements and ensure that the information available is useful for participants. The results of a survey that examined the information security sharing utility of available information types for small and medium organizations is presented in Figure 3-5. Clear preference was demonstrated for certain information types by small and medium enterprises. While there are information types that are highly useful, sharing is still not achieved since the environment perceives the act of sharing as risky in some instances.

Interest in information sharing among small businesses is a relatively new development, but the practice is more established between larger businesses. Larger corporations have attempted to share information in prior years but has found that the information made available is insufficient. In addition, an abundance of tools and threat intelligence information is available to organizations, but these are not perceived as useful. A general impression regarding shared or purchased data is that the data once received is often too old to be actionable (Ring, 2014).

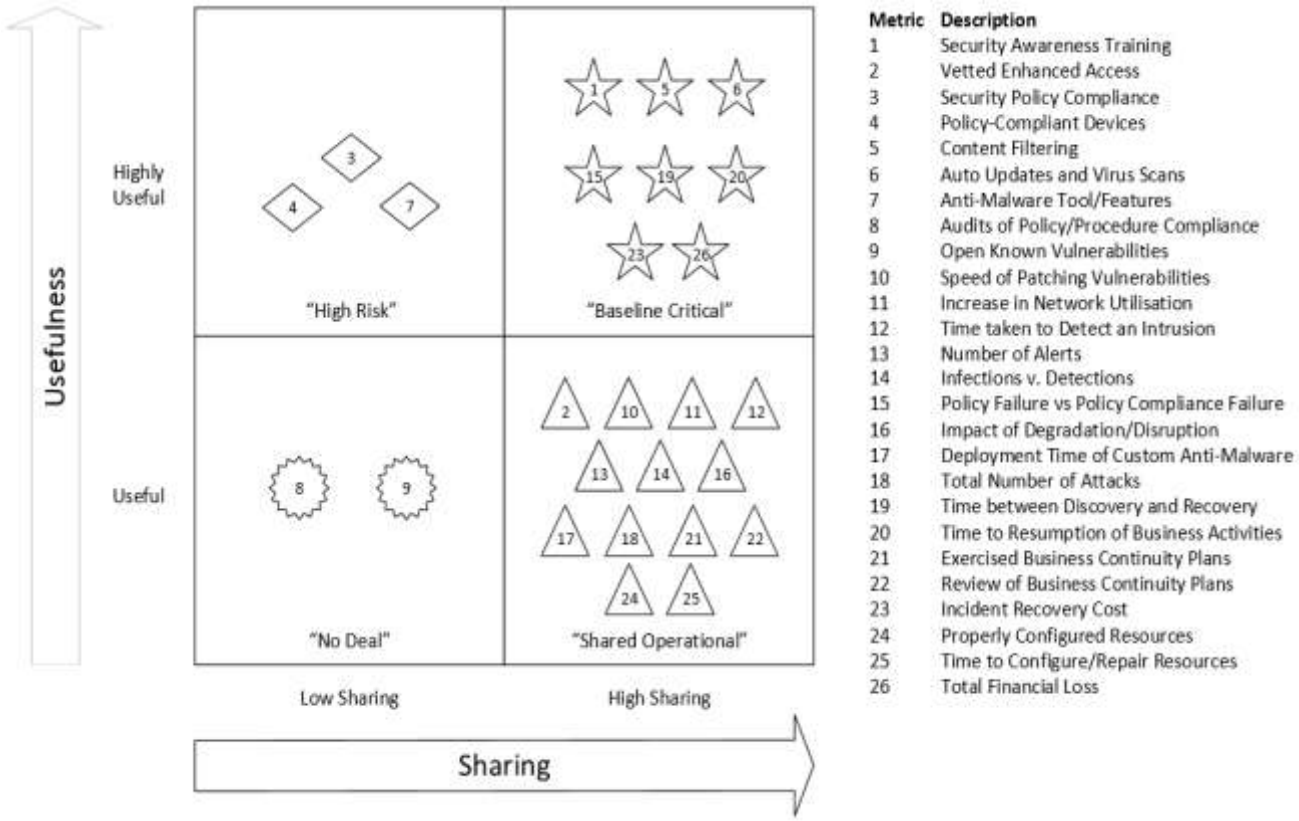

Figure 3-5: Utility of shared SME information (Lewis et al., 2014)

Information sharing is thus not a trivial undertaking, it requires actionable intelligence delivered to the right organization in a sufficiently short period of time that action can be taken. The terminology commonly used for such information is pro-active security information but various possible architectures exist for sharing at national level (Beaudoin, Gregoire, Lagadec, Lefebvre, Luiijf & Tolle, 2010). The following section will discuss the principles of pro-active security and compare it with traditional reactive security.

3.4 PRO-ACTIVE VS. REACTIVE SECURITY

Security can only really exist if there is adequate time to respond to a threat (Berghel, 2007). Considering this statement, the assumption can be made that pro-active security is the only real security. Unfortunately it is also impossible, or at least highly improbable, to anticipate all events that could impact on security. Reactive security is thus also a vital component in the struggle to maintain security. The balance between the two approaches have been the topic of discussion for a considerable amount of time. Determining what strategy to use is difficult since empirical evidence is available to

support either strategy. Research proving that pro-active strategies seem to result in lower losses is available (Kwon & Johnson, 2014). Similarly, proponents of reactive strategies have formalized models that show the superiority of the reactive approach over the pro-active approach (Barth, Rubinstein, Sundararajan, Mitchell, Song & Bartlett, 2010). The argument for implementing a reactive strategy is simply that the initial cost of a pro-active implementation typically requires a large initial economic expenditure. In addition, reactive strategies might be faster since the defenders are only looking for security breaches as opposed to breaches that might not even have occurred. Careful consideration should be given to the requirement of the operational needs since the creation of a reactive capability requires a different approach when compared with a pro-active capability (Baskerville, Spagnoletti & Kim, 2014).

An example of pro-active security is found in the manner in which CERT[13] handles vulnerabilities that could affect critical infrastructure. Sharing of information to affected partners occurs immediately once the responsible vendor has been informed. This approach provides affected organizations with the ability to implement a mitigation strategy for the attack through other technical means until a patch is released. Unfortunately as a side effect, this de-incentivizes the responsible vendor to release the patch, since the potential security risk has been mitigated (Cavusoglu & Raghunathan, 2007).

3.5 PRO-ACTIVE DETECTION LIMITATIONS

The motivation for pro-active security must consider the speed with which a network or resource on the Internet can be attacked with. Even a real time monitor might not provide enough reaction time to respond to a threat. In fact, any solution to effectively prevent and detect attacks on monitored infrastructure with absolute accuracy would require a monitoring network that is faster than the network the monitored resource is connected to (Bass, 2000). An example of such a sensor network is depicted in Figure 3-6.

[13] http://www.cert.org

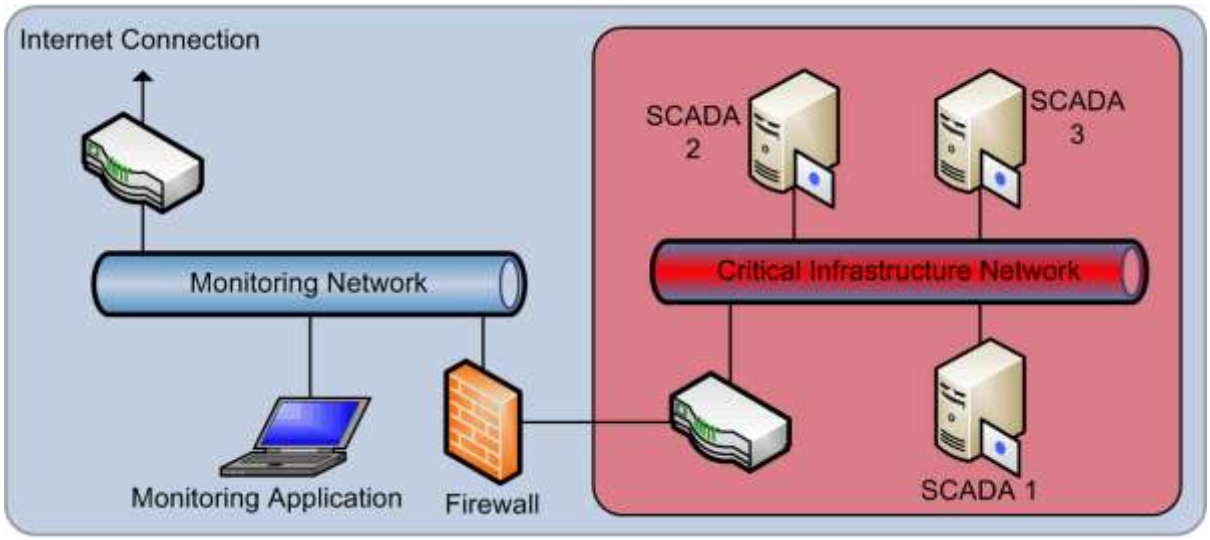

Figure 3-6: Critical infrastructure and monitoring sensor network

This approach increases monitoring and response capability but has implications for attack prevention. By lowering the speeds of the network the critical infrastructure operates on, it compounds implications for the reactive device endpoint security. The typically lower processing power of the devices classified as critical infrastructure makes current security implementations an already complicated task. Adding to these limitations that already include processing power and network speeds that force researchers to explore alternatives such as quantum encryption solutions that significantly increase costs (Hughes, Nordholt, McCabe, Newell, Peterson & Somma, 2013). The experiments making use of quantum cryptography typically require fiber optic links for transmission, thus mandating a centralized type structure. This is not an ideal situation since making use of land line cables might not be the best implementation strategy due to the typically centralized structure of telecommunication centers. A centralized structure typically has a single node of failure that might not be ideal for critical infrastructure.

As an alternative, wireless sensor networks have been proposed for their low cost and potential attack survivability (Buttyán, Gessner, Hessler & Langendoerfer, 2010). This will allow the pro-active defense network to still operate and increase the internal network robustness. It has the potential added benefit that depending on the network topology selected, a large part of the network might remain operational even after a part of the network has been taken down in an attack. While the technology might be ready for commercial use, several security considerations need to be addressed before it is implemented in critical infrastructure protection. Operational challenges such as

integrity, security considerations and communication speed all pose significant implementation challenges (Chen, Díaz, Llopis, Rubio & Troya, 2011).

Both pro-active and reactive strategies have clear potential to contribute to the defense of protected infrastructure. When combined with the need for information sharing as discussed in Section 3.3, pro-active sharing can help defenders to place reactive defenses in time to stop attacks. While voluntary information sharing is key to gaining insight into organizations either in similar industries or in the same geographic regions, there are a variety of other data sources that could be used to pro-actively defend against attacks. The following section will discuss open source intelligence potential and applications.

3.6 Open source intelligence

Open source intelligence (OSINT) is and established paradigm and has been used extensively in a variety of fields. Examples of open source intelligence utilization can be found in the USA's war on drugs (Holden-Rhodes, 1997), research data collected to monitor climate change (Malone & Klein, 2007), and even detection of flu outbreaks worldwide[14]. The cyber security field has also in prior years benefited from the growth of potential information sources in open source data sets: for example information regarding infrastructure or operational procedures. Social media data mining has also been extensively explored and proven their potential. Applications making use of open source social media data have been used in experiments to determine if individuals have negative feelings against law enforcement or to detect dissent (Gritzalis, 2014). This type of research has the potential to identify insider threats, thereby reducing the potential impact of a security breach by limiting access to resources.

The potential impact that open source intelligence can have on a national level is immense, and the utility of open source intelligence has already been demonstrated by Glassman and Kang (2012) when it was applied at organization level. In publications detailing the future requirements for Computer Security Incident Response Teams (CSIRT), awareness is a clear requirement. This increased situational awareness has to include open source datasets as well as information sharing between partners (Ruefle & Murray, 2014).

[14] http://www.google.org/flutrends

It is not just at a cyber security response team level where the need for better open source intelligence is recognized. Governments are increasingly aware of the potential that open source intelligence has. While open source data contains the information, it very often also leads to information overload due to the sheer volume of information available. To address this, both the USA[15] and Switzerland have created open source intelligence data centers (Pallaris, 2008). Other examples of open source intelligence usage comes from law enforcement that aims to better utilize information available about crimes that were committed to respond faster (Brenner, 2004).

The application of open source intelligence is not just a defender paradigm, attackers also extensively make use of open source information to profile potential targets. For example, the terrorist group Al Qaeda stated that open source information can provide as much as 80 percent of required information on a specified target (Weimann, 2004). This sounds like an unrealistic assumption but subsequent research attempting to verify this statement indicates that eighty percent is a conservative estimate. In a number of instances, a hundred percent of required information to successfully attack a target was obtained from open data sources (Brown, Carlyle, Salmeron & Wood, 2005). This is due to the variety of data available in open source data sets which can range from infrastructure details to personal information or even passwords in some instances. Chapter 4 examines a variety of data sources in more detail.

Open source data thus has the potential to be a double-edged sword. It is both useful to the attackers and to the defenders in the sense that information relating to a target is available. From the defenders' side, the information can be used to strengthen disclosed vulnerabilities, and from the attackers' side, it provides enough information to plan an attack. However open source data is also difficult to process: it is in many instances unstructured and requires processing to extract the relevant information from it. Recognizing this potential threat, the USA based Defence Advanced Research Projects Agency (DARPA) has made available funding for research to address and find effective open source intelligence from open data sources[16].

Several examples show how open source data can be used in conjunction with proprietary data to gain effective results. In work performed by Cadariu (2014), the combination of vulnerability databases to create an alert system has received good feedback from commercial role players. Instances are described where security

[15] https://www.opensource.gov
[16] http://www.sbir.gov/node/411192 Proposal number SB133-002

personnel only became aware of vulnerabilities affecting their systems through the experimental system. This resulted in a situation where customers placed vendors under increased pressure to resolve the known, but uncorrected vulnerabilities. Another experiment made use of open source data to verify security vendors' claims that phishing sites were removed within a period of four to five hours (T. Moore & Clayton, 2008a). It was shown that the vendors were overly optimistic: the experiment's revised estimates for website takedown were in the range of 62 – 95 hours. The experiment also highlighted how the lack of information sharing between phishing trackers, increased losses by slowing down detection.

Bianco's work, discussed in Section 3.3, presented the pyramid of pain that illustrates how information sharing can increasingly slow down attackers by denying required information. The slowdown of attackers is achieved by either sharing information with collaborating partners or by examining open source datasets for indicators of compromise. Chapter 4 discusses additional benefits of these open-source datasets. Open source research is also available in the field of critical infrastructure. Several instances of critical infrastructure protection initiatives making use of open source data, such as Shodan, has been documented (Leverett, 2011; Williams, 2014).

The simple fact is that the potential use of open source information on a national leval has only been explored in a cursory manner. Several underutilized sources of data are available to address serious security issues that could significantly impact on a nation. One potential example is the continuous rise of information security breaches. Protecting PII is key for any organization not just because of legislation, but due to the potential misuse of the obtained information. These breaches occur on all levels, both commercial and governmental making no single sector immune. Figure 3-7 illustrates the variety of both size of data breaches and variety of sectors affected. The image presented uses the size of the breach, to indicate the number of records lost. The data breaches presented in Figure 3-7 are only those that have been captured by the website authors, many more exist. The South African police service data breach that occurred in 2013 is located in the upper right hand corner of Figure 3-7 next to the Living Social and Yahoo Japan breaches. Another notable South African incident, is discussed in Section 4.4.8 and does not appear to be listed in this data source. Both the data and the manner in which it is presented is important and Section 3.7 will provide a brief introduction into information visualization.

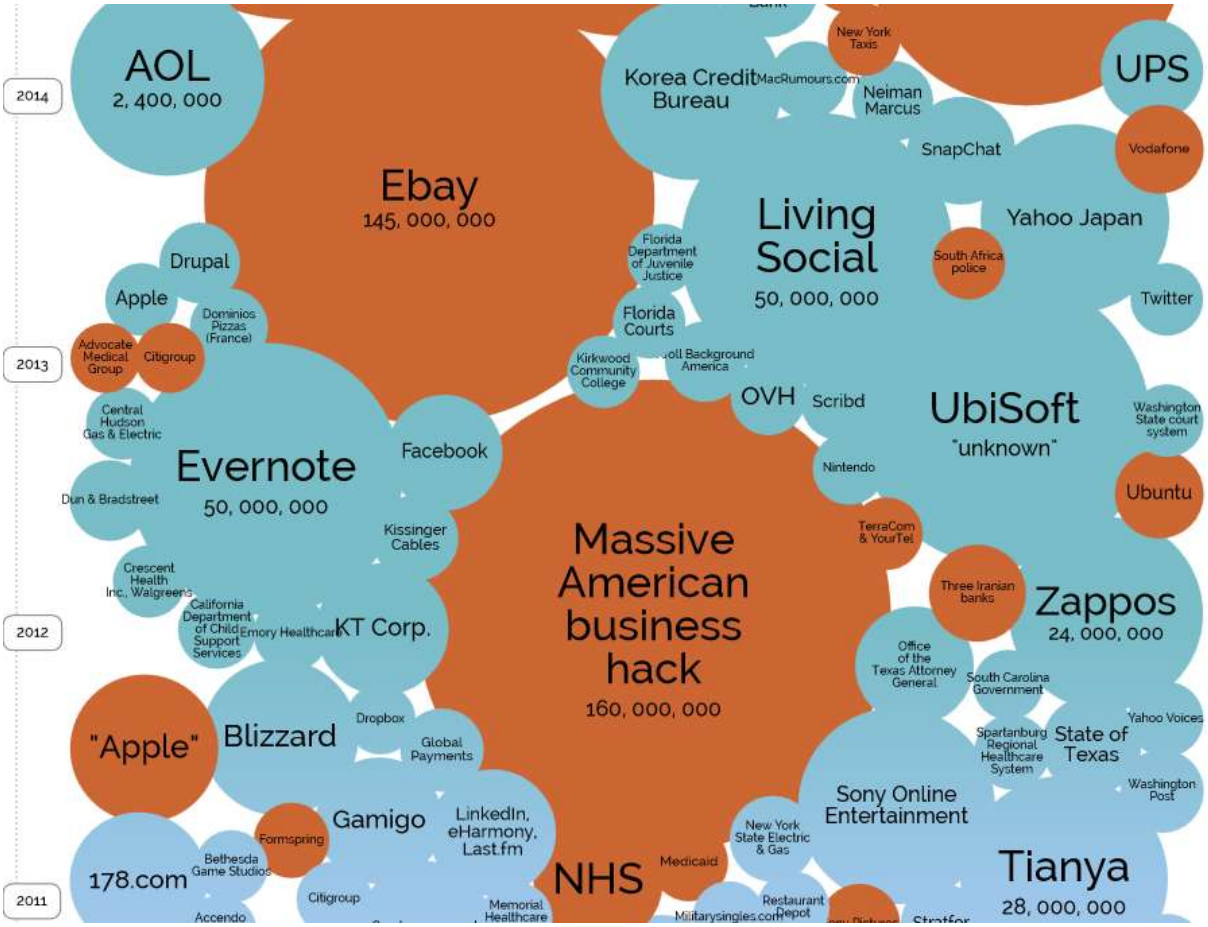

Figure 3-7: Data breaches visualized per breach size[17] on 2014-10-21

3.7 VISUALIZATION OF INFORMATION

The most prominent factors limiting information sharing listed in Table 3-1, indicates either a lack of relevant information or a lack of ability to effectively process the information. While the lack of information might be supplemented with open source data, as described in Section 3.6, the need for effective information processing remains. Cyber sensors typically provide information in textual form creating an abundance of data. This abundance of textual data is typically simply too much for humans to evaluate effectively and tends to overwhelm instead of aid the analyst (Davey, Mansmann, Kohlhammer & Keim, 2012). What is thus required are generic platforms to process complex data in such a manner that the human operator is able to comprehend the situation.

Visualization of information to assist operators to understand data rich environments quicker has previously been documented (Bertini & Lalanne, 2009). The increase in

[17] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

comprehension is understandable considering the research performed by Grady (1993) in human vision. The research indicated that 30% of the human brain is allocated to sight, with the next highest sense touch, achieving only 8%. While making use of visualization sounds much like common sense, the information environment often has multiple stumbling blocks preventing effective visualization (Marty, 2009). Work performed by Card, Mackinlay and Shneiderman (1999), describes the process required to transform raw data into a task that a human operator easily comprehends. The process requires the transformation of data from a raw format, into a structured format that should then be mapped to visual structures based on human understanding. From there it should be presented to the user as Figure 3-8 illustrates.

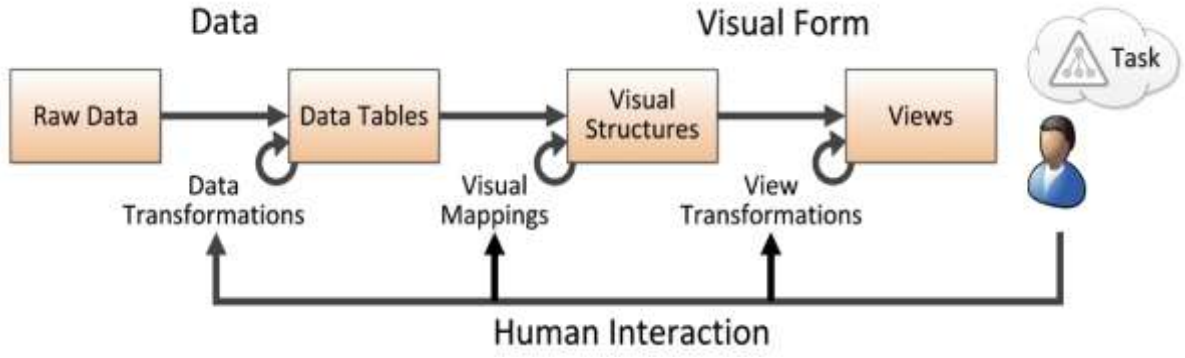

Figure 3-8: Information Visualization Pipeline (Card et al., 1999)

3.8 SUMMARY

This chapter built on the information presented in Chapter 2 and examined in finer detail what the potential attack surface of a nation could be represented as from an attackers perspective. The chapter discussed how the amount of energy required from the attacker could be increased, by denying or sharing certain key pieces of information. Other key concepts that can be used to gain a deeper understanding of the described attack surface were introduced such as: pro-active vs. reactive security, control of open source intelligence and visualization fundamentals..

Chapter 4 will build on the information provided in this chapter by examining several sources of information related to information security on a national level. These sources will be examined and evaluated for accuracy, applicability and usefulness to address common information security problems affecting a country.

National borders aren't even speed bumps on the information superhighway.

Timothy C. May – Senior scientist at Intel

4

Examination of data sources for use on a national level

4.1 INTRODUCTION

Previous chapters have examined the need for national cyber security programs and discussed the potential contribution information sharing and open source intelligence could provide. To facilitate sharing, several sources of data are already available to information security researchers that are applicable not only to organizations but also to nations. These data sources tend to be either provided by a commercial third party or via voluntary aggregators. Since the Internet infrastructure is not controlled by any single entity, there is no single network that contains all the required information. Even governmental organizations interested in national infrastructure can only obtain information regarding infrastructure directly connected to their own networks. Unless there is some form of control delegated or permitted from internal organizations, the distributed nature of the Internet mandates collaboration to obtain a clear view of deployed systems and infrastructure. These types of co-operation agreements are typically hard to come by since it has been well documented that obtaining information security data is a significant undertaking due to the personal nature of the data (Kotulic & Clark, 2004).

Even with collaboration in place, a variety of factors exist that limit researchers' ability to create effective processing techniques for the available data sources. Availability of data and more importantly, the lack of output standards applied uniformly across these data sources (Marty, 2009), are a significant limitation to effective processing. With well over a thousand information security standards published and potentially in use (PwC UK, 2013), there is no single dominant standard and even less of a standard for the output provided by systems in the form of log files, reports or database entries. Add to that the complex ecosystem of the Internet, with a myriad of different programming languages, number representations, language and regional differences, and it becomes a near impossible task to effectively make use of just the available information security datasets to obtain a clear view.

Cyber sensors have already been mentioned in Table 3-1 as a crucial component required to gain insight into the cyber domain. A cyber sensor does not have any specific form, it can be a network telescope or a Raspberry Pi, as long as the sensor provides the potential to gain increased situational awareness in the cyber domain or aspects related to the cyber domain (Otis, 2013). This chapter examines a subset of the more prominent data sources available on the Internet that could potentially act as cyber sensors. The examination is by no means a complete taxonomy of all available information security data sources. The sources discussed were considered for use in the construction of a experimental data fusion system that will be discussed from Chapter 5 onwards. The focus of the examination is on the data sources, the type and volume of data they provide and their limitations. Examination will occur by means of specific literature reviews and limited case studies where applicable. The level of detail provided is crucial to illustrate the types of flaws present in basic data sources that could be used as sensors for cyber security situation awareness.

4.2 STRUCTURE AND LOCATION OF POTENTIAL INFORMATION SECURITY DATASETS

While the question regarding who controls the Internet has been asked before, it is clear that a number of parties control the Internet – the numerous operators that provide the cabling infrastructure between continents, such as Seacom[18], SAT3[19] or WACS[20]; the Internet registrars that make sure that the DNS entries reflect back to the correct IP address, such as the .co.za[21] domain registrar in South Africa. While it is true that all of these entities control certain aspects of the Internet, they do not control the entire Internet. National government might be able to control the DNS registrar (the main link between countries via the main ISPs) through the use of legislation, but they do not own the infrastructure required for communication.

In Figure 4-1 the simplified structure of the Internet is depicted. Should any party wish to obtain a full view of the systems and infrastructure, the co-operation of a number of parties will be required. Consider that government will have access to its own networks, but not the networks of the ISP that it is connected to. Nor will government have information regarding the inner workings of the corporate client connected to the same ISP that government make use of. To obtain a full view of all devices, software and personnel, the co-operation of both the ISP and the corporate clients will be required.

[18] http://seacom.mu
[19] http://www.safe-sat3.co.za
[20] http://wacscable.com/index.jsp
[21] http://co.za

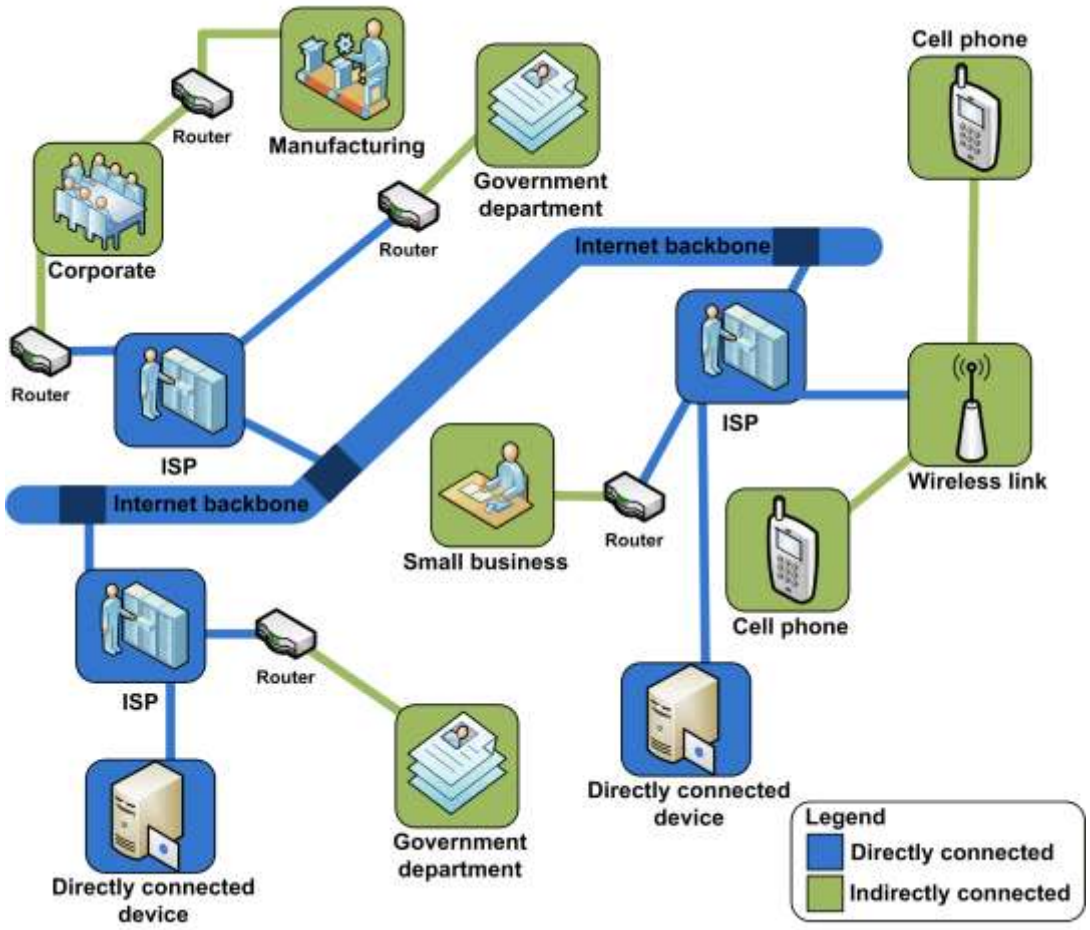

Figure 4-1: Simplified structure of the Internet

At any given point there is only a limited set of organizations that could potentially have access to information relating to systems and infrastructure. Thus, while the decentralized nature of the Internet is a significant benefit for the reliability and fault tolerance of the system, obtaining a clear view presents a complex problem for any single organization. Due to the distributed and de-centralized nature of the Internet a variety of parties are more active in certain areas than in other. Often these third parties will allow the information collected by their systems relating to their specific aspect of the Internet to be purchased, such as that available from Shodan[22]. At other times there is no fee involved but instead the third party can choose to share the information to the information security community or not. An example of an important sharing effort is the contribution made by the United States government in the hosting and distribution of the National Vulnerability Database[23]. No registration or fee is required to obtain the data contained in the library and it is available to everybody for their own use.

[22] http://www.shodanhq.com
[23] http://nvd.nist.gov

In Figure 4-2 a snapshot of the Internet of 2010 is presented to depict just how significant the scale of the Internet has become. The higher the intensity of the image, the more concentrated the location of the devices as they are grouped by IP range.

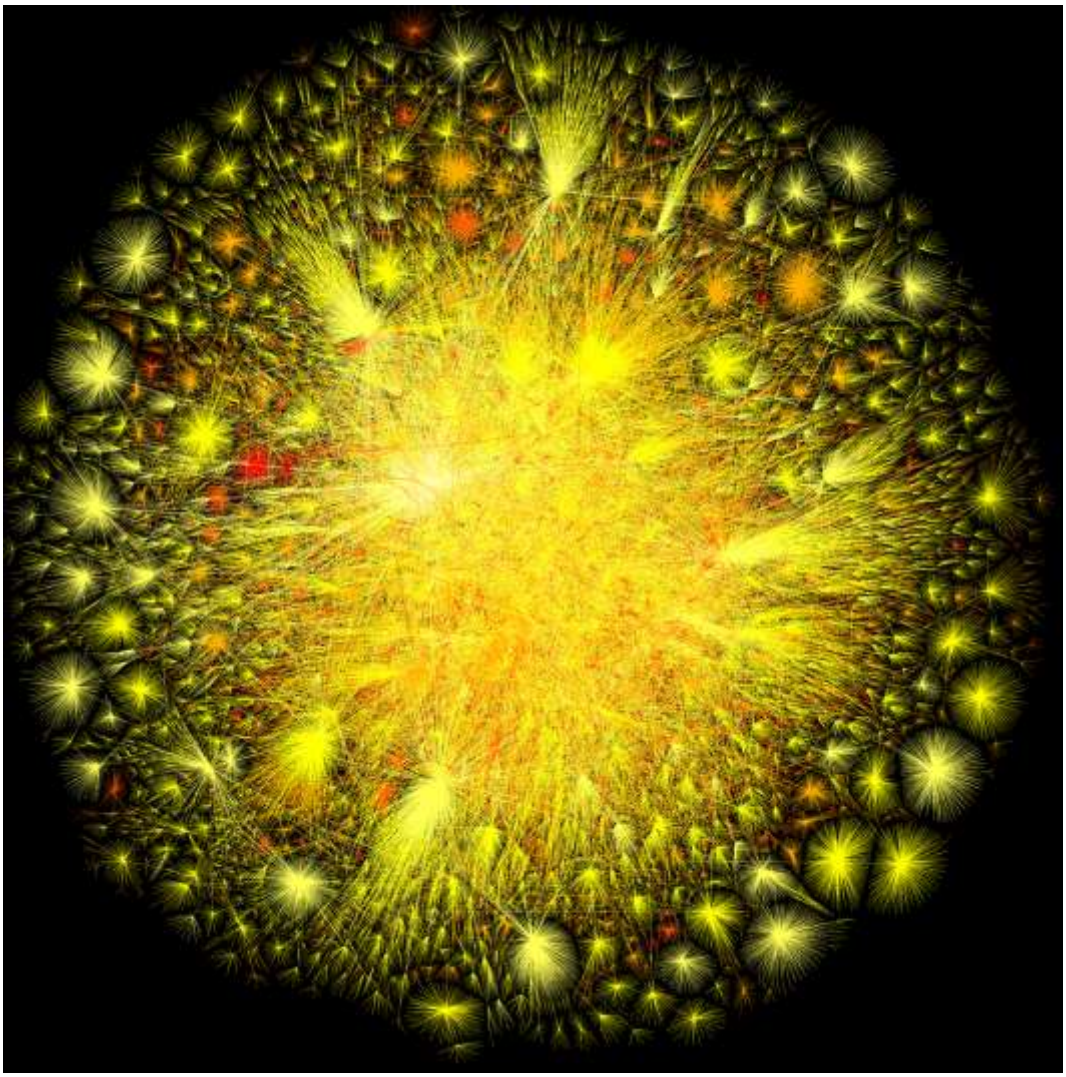

Figure 4-2: Visualization of the complete Internet in 2010 from the Opte Project[24]

The image in Figure 4-2 is generated by the Opte Project[24] that used Border Gateway Protocol (BGP) routing to determine routes available between devices. It is currently estimated that the Internet contains 1.85 billion pages as calculated on 2014-07-14 from the work performed by De Kunder (2008) in his project WorldWideWebSize[25]. This measurement is just human viewable web pages and does not include the multitude of web services, dedicated computing platforms or connected embedded devices. The various data sources and their individual potential will be discussed in more detail from Section 4.3 onwards.

[24] http://www.opte.org/the-Internet
[25] http://www.worldwidewebsize.com

4.3 DATA SOURCES

Section 4.4 and 4.5, examines commercial and freeware datasets available from third parties. Depending on the methodology and data set obtained, a data set may hold information regarding a single organization or the entire Internet. The information sources range from commercial to private entities and as such the data contained in the datasets will inherently vary in accuracy, method of representation, measurement and a variety of other significant factors. Some sources cannot strictly be seen as sources since they are aggregators of a variety of different data feeds. The examination of each data sources varies in detail and length only due to the purpose of the investigation. Some data sources might provide detailed datasets that need to be investigated for accuracy and relevance that will require additional content and discussion.

The data sources discussed will be grouped into one of two categories depending on the type of data that the source describes. Data sources that directly describe objects related to the attack surface of a nation (discussed in Section 3.2) such as infrastructure devices, software or people will be placed in one group. Datasets that do not describe a specific object but rather provide more detail regarding the attributes of the object will be placed in the other category. The categories are labeled object datasets and metadata datasets and discussed in more detail in Section 4.4 and 4.5 respectively. These data sources will be evaluated for usablility in the research in Chapter 5.

4.4 OBJECT DATASETS

The data sources listed in this category can be used to provide a view of the objects present in the cyber domain. The information sources discussed in this section typically report information regarding a specific object by means of an IP address, name or unique identifier. While the data sources discussed typically also contain additional data regarding the Internet object, the focus is always on the specific object, not aspects related to the object.

4.4.1 BUILTWITH

Obtaining information regarding the types of software frameworks and components used to construct company infrastructure is very useful for attackers. Previous work noted that Content Management Systems (CMS) are a breeding ground for vulnerabilities (Shteiman, 2014) due to the attractive target they present to attackers. If a vulnerability in a CMS is discovered, the odds are high that the vulnerability will be exploitable on a significant number of machines with the same version of software and

infrastructure setup. This will allow an attacker to gain access to a potentially vast number of systems in comparison to a single system with a unique vulnerability.

The company Builtwith[26] specializes in examining as many as possible publicly available web pages and attempting to identify the development technology used to construct the web page. A significant number of systems have been indexed but the site provides the ability to examine a custom site via a simple query. Details provided in the return set are comprehensive and document usage from elements such as the type of web server used to deliver the content, CMS version used and specific details regarding web technology such as HTML, JavaScript or Style sheets used. Frameworks used such as PHP, Ruby on Rails and Django are reported in great detail with specific version number, and modules installed detected. Security features such as Secure Socket Layer (SSL) certificates detected (and each certificate's registering authority), is also provided, along with any custom search or aggregation functionality contained in the website.

While it is useful to detect the types of technology used in web portals, Builtwith also provides the ability provided to search by technology platform, returning a list of all relevant domains. This is arguably of more importance from a defenders point of view. Should a specific web technology vulnerability be discovered, a query could link the national CERT with a list of all the websites that contain the vulnerable software.

Obtaining data from Builtwith is only available via online application programming interface (API) with no bulk download option. Neither do they provide bulk extracts of domains a customer has a specific interested in. Thus, to effectively make use of the Builtwith API a consumer would first require a list of all registered South African domain names. Obtaining such a list is not possible at present without Governmental or legal requisition and it is for this reason that Builtwith was not considered for this study.

4.4.2 SHODAN

Shodan was created by John Matherly in 2009 and has been described as '*the search engine for hardware devices*' (O'Harrow Jr, 2012). The service allows an individual to search for devices connected to the Internet in a variety of ways such as vendor, operating system, specific ports utilized by the hardware or even country code. The devices detected are typically Internet-facing devices and it will be irregular to detect devices such as mobile phones, since these devices are typically behind a mobile

[26] http://builtwith.com

operators network gateway. Mobile devices are not immune to detection or tracking, but due to their limited direct exposure to the Internet the identification techniques often require the interaction of the user (Bojinov, Michalevsky, Nakibly & Boneh, 2014). Shodan retrieves a variety of information from the device and attempts to keep a history of devices detected on the Internet. This is useful due to the nature of the Internet where a multitude of devices make use of temporarily allocated IP addresses.

The system has in recent years been used extensively in academic and private research, for example by Leverett (2011) in their work to detect, visualize and assess critical infrastructure types and vulnerabilities. The service relies on artifacts such as banner type which has previously been proven possible by Caselli, Hadžiosmanović, Zambon, and Kargl (2013). The Shodan project's ability to provide data regarding the devices the Internet is operating on is of tremendous importance. While it is true that software vulnerabilities are still the most dominant form of attack vector, attacking the hardware has recently become significantly more likely. Hardware attacks have been extensively researched and while physical access to a device is often required, there is a variety of attacks, such as timing attacks, that could potentially be performed over a network connection (Karaklajić, Schmidt & Verbauwhede, 2013). CVE lists already contain vulnerabilities that affect hardware devices, and with the aid of Shodan, defenders can obtain insight into the devices under their control exposed to the Internet.

With the newly acquired ability to detect exposed devices, research has shown that it can reduce the discovery time of devices and help with protection of critical infrastructure (Hansen, 2012). Military research has also illustrated the significance of this type of work: Otis (2013) describes how Shodan can serve as an independent sensor in the military environment. The ability to effectively assess inventory from an independent source is potentially crucial for defenders. Hardware equipment bought from vendors are typically placed in data centers and other sensitive areas and it is out of the realm of possibility for many defenders to perform security audits on devices on firmware and chip level. Vendors may reuse a variety of components from one product to the next and if a vulnerability is detected, the ability to examine available systems could identify more devices affected than just those presumed by the vendor.

There is not only the potential for defense with the Shodan data but also the potential for attackers to increase their knowledge regarding the infrastructure of their potential victims. Should an exploit become publicly available, Bhatia et al. (2014) has proven that Shodan allows operators to search for exact match devices. In the research a search

for smart televisions were conducted. With geolocation, the researchers could determine what type of smart televisions were most used in which geographic region. The potential to misuse this type of information is always a reality.

Obtaining data from Shodan is a highly configurable process, and the data is available in both API or bulk download format. Purchases are instant, and for a modest fee a variety of additional filters are available. These additional filters such as the ability to filter by country ensures that only required data is purchased.

4.4.3 BLACKLISTS

Domain blacklists are lists that contain the domains that have been detected as unsafe by a variety of different contributors. These blacklists provide system administrators with the ability to block certain domains on a proxy level to protect their internal users. Firewalls and proxy devices can even be configured to update these list automatically as they are published from a variety of vendors. These lists are not foolproof and in specific circumstances, completely legitimate domains names can incorrectly be included. It should therefore not be seen as a definitive indicator of a malicious domain, but rather as a suggestion that the domain might be malicious.

Dshield[27] provides these types of blacklists and categorizes the severity of the detected site according to a low[28], medium[29] and high[30] classification schema. Performing a search on the Dshield dataset for any .co.za domain produced only 29 results for the time period 2000-01-01 to 2014-06-01, displayed in Table 4-1. Once a domain is removed from the active list, the classification is no longer available, as indicated by the dash.

Thus, the Dshield list at the time of writing has four active domains for South Africa that it considers as suspicious. This is a remarkably low number considering the growing size of the South African Internet domains and the number of registered domains as stated by the .co.za registrar. The current number of .co.za domains registered as stated by the .co.za registrars is 959364 on 2014-06-01. Given that only 4 domains were identified as malicious, the data could be wrongfully interpreted to state that 99.9 percent of all websites in South Africa are trustworthy.

[27] http://www.dshield.org
[28] https://isc.sans.edu/feeds/suspiciousdomains_Low.txt
[29] https://isc.sans.edu/feeds/suspiciousdomains_Medium.txt
[30] https://isc.sans.edu/feeds/suspiciousdomains_High.txt

Table 4-1: Dshield[27] malicious .co.za domains during 2000-06-01 and 2014-07-01

	Domain	Suspicious Status
1.	abbott.u4ria.co.za	_
2.	anilaba.co.za	_
3.	arizonaguesthouse.co.za	High
4.	bobbo.co.za	_
5.	brokersearch.co.za	_
6.	cmengineers.co.za	_
7.	cmgsolutions.co.za	_
8.	ddcsa.co.za	_
9.	digitearlandroid.co.za	Medium
10.	donorlife.co.za	_
11.	ftp.sinosa.co.za	_
12.	genius.cellc.co.za	_
13.	geraldinesstudio.co.za	_
14.	gooi.co.za	_
15.	havemercyworld.co.za	_
16.	infinnitiesprom.co.za	_
17.	jorpe.co.za	High
18.	kopa.co.za	_
19.	nawaopls.co.za	_
20.	onlinepayroll.co.za	_
21.	pepkorcd.co.za	_
22.	toringkerk.co.za	_
23.	www.delmontcaldowcaterers.co.za	Low
24.	www.everythingwritten.co.za	_
25.	www.fillmyfum.co.za	_
26.	www.iamgm.co.za	_
27.	www.mavin1ok.co.za	_
28.	www.property-jds.co.za	_
29.	www.ssisco.co.za	_

MalwareDomains[31] is another service that offers an updated list of domains reported as being malicious based on a variety of data sources. Data sources include Google Blocklists, community contributions and the site's own active scanning. The list in Table 4-2 as obtained on 17 June 2014 contained only eight .co.za domain names.

Table 4-2: MalwareDomains malicious domains detected in .co.za domain[31] on 2014-06-17

Domain	Risk	Date Detected
cwgc.co.za	High-Risk	2013/10/18
arizonaguesthouse.co.za	Harmful	2013/11/23
sigrotec.co.za	Harmful	2013/12/04
jorpe.co.za	Harmful	2013/12/19
bisselltraining.co.za	Harmful	2013/12/26
glochemslaboratory.co.za	Scam	2014/01/05
www.visitknysna.co.za	Malicious	2014/01/17
fuckmate.co.za	Browlock	2014/02/04

There are a number of lists that contain information regarding domains that host malware, are involved with scams or sending out spam e-mails. Currently no single source is the dominant standard and as a result list aggregators have started to offer a variety of the most prominent lists in a subscription based format. One such aggregator is the Malware Patrol[32] aggregator. It provides a wide variety of block lists and updates them automatically for user download on a regular basis as shown in Figure 4-3. Depending on the type of service selected, a user can expect hourly updates on the professional plan or updates every 72 hours on the freeware version.

[31] http://www.malwaredomains.com
[32] https://www.malwarepatrol.net

URL block lists/feeds

	Regular List	Aggressive List
BIND like DNS Servers	N/A	Please upgrade
Carbon Black 4.1+ (domains)	N/A	Please upgrade
Carbon Black 4.1+ (MD5 hashes)	Please upgrade	N/A
ClamAV Virus DB (basic)	Download	Please upgrade
ClamAV Virus DB (ext)	Please upgrade	Please upgrade
DansGuardian	Download	N/A
Firekeeper 0.2.9 or newer	Download	Please upgrade
Hosts file - 127.0.0.1	Please upgrade	Please upgrade
Hosts file - 127.0.0.3	Please upgrade	Please upgrade
Hosts file - 0.0.0.0	Please upgrade	Please upgrade
Hosts file - MacOS pre OS-X	Please upgrade	Please upgrade
MailWasher block filters	Download	N/A
MaraDNS - CVS2	N/A	Please upgrade
MD5/SHA-1 hashes	Please upgrade	N/A
Microsoft DNS Server	N/A	Please upgrade
Mozilla cookie filtering	N/A	Please upgrade
Mozilla Firefox AdBlock	Download	N/A
Plain text	Please upgrade	Please upgrade
Postfix MTA	Download	N/A
SmoothWall	Download	N/A
SpamAssassin	Download	N/A
Squid Web Proxy ACL	Please upgrade	Please upgrade
SquidGuard	Please upgrade	N/A
Symantec Security for SMTP	Download	N/A
Symantec WebSecurity	Download	N/A
XML	Please upgrade	N/A

Figure 4-3: Malware Patrol block list aggregator available list feeds[32] on 2014-06-17

The information contained in the list is the freeware version and as such not all information is available. Content only available for premium subscribers are marked with the "Please upgrade" text. The list contains a wide variety of data sources but there are still a number of sources not provided. Specialized botnet detector trackers such as the Zeus botnet tracker provides up to date information on domains the botnet communicates with and is extremely relevant as can be seen from the Command and Control (C&C) server located in South Africa on 2014-06-01 shown in Figure 4-4.

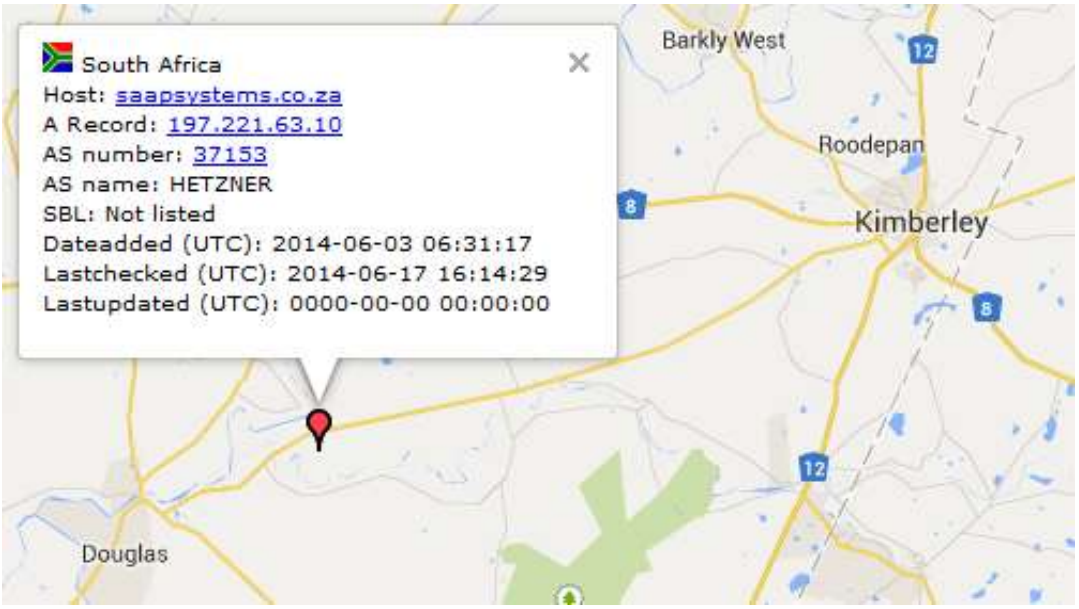

Figure 4-4: Zeus Botnet Command and Control infrastructure detection[33] on 2014-06-17

Thus, to establish a truly accurate picture of the situation in South Africa, a system would need to download and process as many as possible blacklist data sources since none are singularly comprehensive.

After downloading and searching for all .co.za domains in the freely available datasets, the results in Table 4-3 were generated. Although a far larger number of blacklists were examined, far fewer results than those of the System Administration, Networking, and Security Institute (SANS) list was obtained. What is important however is that there are different results obtained than those detected in the SANS list available in Table 4-1.

Table 4-3: Malware Patrol .co.za detected domains block list on 2014-07-17

Domain	Smoothwall	Symantec	Dans Guardian
www.pricepointit.co.za	X	X	X
wokini.co.za/modules/mod_araticlhess/pdf_sepa	X	X	X
nedlimited.co.za	X	X	X

Yet another implementation of detecting malicious domain names is that of the online entity Xylotil who created the site Cyber Crime Tracker[33]. The site claims to be dedicated to the tracking of botnet C&C infrastructure. Correlating these URLs in the database reveals that at least four different types of command and control servers were hosted in the .co.za domain as listed in Table 4-4.

Table 4-4: Cyber Crime Tracker detected Command and Control URLs[33]

URL	C&C Type
www.everythingwritten.co.za/images/tm/cp.php?m=login	Zeus
cvcoal.co.za/mail.php	Mailer
cvcoal.co.za/img/logs.php	WSO
www.property-jds.co.za/files/adm/index.php?m=login	IceIX
www.property-jds.co.za/web/adm/index.php?m=login	IceIX
biterelish.co.za/txt/cp.php?m=login	Zeus
www.delmontcaldowcaterers.co.za/templates/system/html/cp.php?m=login	Zeus
artofsklncare.co.za/admin/mmbb/mmb/mmbb/cp.php?m=login	Zeus
broncobearings.co.za/vices/cp.php?m=login	Zeus
st-andrewsspa.co.za/bmg/cp.php?m=login	Zeus
saapsystems.co.za/ipray/cp.php?m=login	Zeus

A variety of blacklist implementations were examined and it is clear from the evidence obtained that no dominant blacklist currently exists. A variety of these lists need to be consulted on a regular basis to ensure as much as possible coverage is provided. Taking into consideration that each set of results obtained by the aggregator Malware Patrol provided the same three domain names, it might be prudent to check a number of lists with the same data rather than simply using an aggregator.

4.4.4 Social Media

The explosion in social media platforms and use across a broad range of communities can potentially be a great source of information for information security researchers. Research work has already established that it is possible to determine the key role players in a given hacker community (Benjamin & Chen, 2012). This type of information can provide an indication of the level of hacker activity in a country or if applied in a different manner,

[33] http://cybercrime-tracker.net/stats.php

could indicate who was targeting the country. Unfortunately Facebook, Twitter, YouTube and other social media sites all represent complex data sources and collaboration between inter-disciplinary research areas is required (Kinder-Kurlanda & Weller, 2014). This adds to the complexity of extracting useful information from any of the above data sources.

Social media also introduced another platform to interact with users and this increased the opportunity for traditional information security problems such as spam to affect these platforms as well. Traditional solutions that functioned in e-mail applications are not always applicable due to factors such as infrastructure differences and thus specialized research is required to combat these attacks (Jin, Lin, Luo & Han, 2011). This is significant since yet to be discussed sources such as PhishTank in Section 4.4.5, will function as long as there is infrastructure and domains to block. A user on Twitter or Facebook makes use of their infrastructure and requires some form of communication to the owners of the infrastructure to block these types of attack.

Despite the complexity, these data sources should not be underestimated. Geolocation is but one type of information available in a variety of these social media data sources and is very useful. The location field is not always available but inferences can be made to the location and true identity of an individual based on their user activities and relationships (Giglietto, Rossi & Bennato, 2012). Social media such as Twitter has also been proved to disseminate news of software vulnerabilities faster than traditional systems such as vulnerability databases (Gopal, Marsden & Vanthienen, 2011).

4.4.5 PHISHING RELATED

PhishTank[34] is an example of a collaborative service where users can contribute suspected phishing site data. The submitted data is presented to active participants to vote if the site is indeed a phishing site or if it is not. This allows the system to present users with a reputability score that they can then use to decide if the site is a phishing site or not. As with any voting based system, the opportunity for bias, manipulation and incorrect conclusions are very real due to the human element involved (T. Moore & Clayton, 2008b). Another service with a degree of similarity is Escrow Fraud[35] where illegal businesses or fake service provider websites are listed. The site does not allow for wildcard search of just the co.za domain, nor does it provide an API from the documentation available on the site.

[34] http://www.phishtank.com
[35] http://escrow-fraud.com

Unlike Escrow Fraud, PhishTank's data is available and updated continuously with either bulk download or API access available. The bulk data download is available in a variety of popular formats such as XML or JSON making the site easy to integrate with existing data sources. A single entry is presented in Figure 4-5 to illustrate the available information regarding a single reported phishing entry in JSON format.


```
"phish_id": "2329033",
"url": "http:\/\/teambuildingworkshops.co.za\/capitec_eft_notice.php",
"phish_detail_url": "http:\/\/www.phishtank.com\/phish_detail.php?phish_id=2329033",
"submission_time": "2014-03-10T14:01:22+00:00",
"verified": "yes",
"verification_time": "2014-03-16T00:15:59+00:00",
"online": "yes",
"details": [{
    "ip_address": "72.9.231.106",
    "cidr_block": "72.9.224.0\/20",
    "announcing_network": "3595",
    "rir": "arin",
    "country": "US",
    "detail_time": "2014-03-10T14:25:40+00:00"
}],
"target": "Other"
```


Figure 4-5: Fields available in the Phishtank dataset in JSON format[34]

The phishing related databases have inspired many information security solutions such as the work conducted by Mao, Li, Li, Wei, and Liang (2013) who created a novel phishing site detector that operates by comparing Cascading Style Sheet (CSS) files. In other work Fahmy and Ghoneim (2011) created a hybrid phishing detector by submitting the URLs in an email against Phishtank and Escrow Fraud[36], to check if it was not directly blacklisted already.

While a more comprehensive evaluation of the data present in Phistank will be presented in Appendix A, an examination of the data available for 2014-06-24 will be used as a snapshot to examine the data available in the dataset. Examining the dataset for this date reveals that it contains 18962 records in total with 51 entries reported as affecting the .co.za domain space. The intended targets for the phishing emails are available as an option when reporting a phishing e-mail and within this dataset the intended targets were reported as mainly international companies as shown in Table 4-5.

[36] http://escrow-fraud.com

Table 4-5: PhishTank 2014-06-24 co.za domain[34] target data

Target	Count
AOL	3
Ebay	1
Google	1
Nationwide Building Society	1
PayPal	3
Santander UK	1
Other	41

In the available records for the co.za domain space, 41 records indicate that the intended target is not clear from the website and is thus listed in the "Other" category. A variety of reasons can be attributed to the large number of other category classifications when the operation of PhishTank is taken into consideration. Anyone can register on the website as a user and will be allowed to submit a URL that is deemed the phishing URL. It is up to the initial reporter of on the phishing website to enter the name of the organization being targeted by the phisher by means of a pre-defined dropdown list. This situation presents an opportunity where either the reporter makes a mistake and enters an incorrect organization as the targeted organization or that the reporter simply does not know who was targeted and enters the phishing entry with the default "Other" target setting.

Upon closer inspection the data presented in Appendix A can be summarized to the following target list presented in Table 4-6. When comparing the results obtained in Table 4-6 with those presented initially in Table 4-5 the amount of "Other" classifications are significantly reduced to 7 instead of the first obtained 41. To achieve this, the author manually investigated each link relevant to the .co.za domain space and a manual examination of the URL in question was then performed to assess the intended target.

Table 4-6: Revised Phishtank data affecting the .co.za domain 2014-06-24

Target	Count	Classification Available
Santander	1	True
Alibaba	2	False
Google, Yahoo, AOL, Windows	14	Individually
BT	1	False
Google	2	True
Google Docs	2	False
PayPal	11	True
Credit Mutual	3	False
Yahoo	4	True
AOL	1	True
MaxNet	1	False
Capitec	1	True
FNB	2	True
Other	6	True

A number of interesting points can be raised from this type of analysis. While allowing reporters the ability to report a phishing URL's target as the "Other" category, it could lead to incorrect classification. On the other hand, forcing a reporter to select a specific target can also lead to fewer submissions of phishing URLs since the process becomes more complicated. In a variety of instances the phishing URL did not specifically target just one organization but setup one page to target a collection of them. Unfortunately there is no option on the reporting pages to specify more than one target and thus, only one target can be reported instead of the whole collection. This type of generalization could most certainly lead to reporting bias if used by uninformed reporters. The data contained clear evidence of phishing activity specifically related to the South African domain targeting two local banks: First National Bank and Capitec. The initial work presented in Appendix A did not reflect this and it is once again a clear indication that reporting of PhishTank data, while useful should not be performed without extensive investigation.

Six instances of the "Other" classification still remained and a variety of factors can explain these. In four instances, the URLs reported as phishing URLs did not lead to a

web page but instead to a directory on a server with no web content presented. While this has been reported as a valid phishing website, it is unclear to the author how this classification was achieved with the available information. In two other instances no screenshot from the PhishTank site is available to prove prior phishing activity nor is there any activity on the reported URL to indicate anything other than normally functioning websites.

Additional considerations when making use of PhishTank data is to consider that the system does not differentiate between URL addresses submitted by users. Multiple reported activity of phishing could all lead back to one instance of actual phishing such as the following:

- http://diketconnection.co.za/googledocss/sss/index.htm was reported as a valid phishing attempt with id 2465337
- http://diketconnection.co.za/googledocss/sss/ was reported in a separate instance with assigned id 2465863

Both of the addresses above resolved to the same index.htm page. While it is possible that one server can be used to host multiple phishing sites, it is also crucial to understand that web server configurations can influence the resolution of web pages located on the server. Other types of duplicates possible in the dataset is where some URLs can be identical in all aspects except the prefixes in the beginning of the URL such as http://www.xyz.co.za vs. http://xyz.co.za . This type of duplication is beneficial in the fact that it will err on the side of caution to catch all possible variations but it will decrease the accuracy of the number of times a specific site was targeted.

A variety of commercial companies make use of the data generated by Phishtank and this is evident in the speed with which a variety of browsers report phishing sites as malicious. Reporting on malicious sites are available even though the URLs were reported only a few hours ago. In Table 4-7 a subset of the results were tested and only one of the reported URLs were not blocked by either Microsoft SmartScreen technology or Mozilla's Firefox web browser technology.

Table 4-7: Microsoft and Mozilla malicious website blockers 2014-06-24

PhishID	SmartScreen	MozillaWeb
2546770	No	No
2545790	Yes	No
2545603	Yes	No
2541841	Yes	Yes
2541677	Yes	Yes
2541398	Yes	No
2540793	Yes	Yes

4.4.6 REGISTRARS

While potentially a great source of information, registrars are typically bound by strict privacy requirements and as such typically only provide information with a court order in volume. While a web service is usually made available to find contact information relating to the owner of a given domain name, the service is not meant for bulk use. The online service also only provides details relating to the person whose domain was entered. While it would be possible to automate such a query, a pre-requisite for such an operation would be a list of all the domain names registered in a certain domain. This list of registered domains are typically only available from the domain registrar to start with, rendering the automation procedure moot as a possible solution. The dominant registrar in South Africa is the co.za[37] domain registrar according to their homepage.

IP addresses allocations for the African continent is controlled by the African Network Information Center (AFRINIC)[38]. The IPv4 addresses allocated and controlled by the AFRINIC organization include the following ranges as stated on their webpage[39]:

- 41.0.0.0/8
- 102.0.0.0/8
- 105.0.0.0/8
- 197.0.0.0/8
- 196.0.0.0/8
- 154.0.0.0/8

[37] http://co.za
[38] http://www.afrinic.net
[39] http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml

AFRINIC is also charged with allocation of IPv6 addresses and the following blocks have been allocated thus far for use[40]:

- 2c00::/12
- 2001:4200::/23

The 2c00::/12 address contains approximately 2^{117} potential IP addresses and the 2001:4200::/23 address range adds another smaller but still significant 2^{105} addresses. This amounts to $2^{105} * 2049$ addresses allocated for the African continent exclusively. To add perspective, consider that the greatest possible number of devices connected to the Internet on IPv4 amounted to approximately 4.29 billion (4294967296). Compared to the amount of devices potentially available under the IPv6 scheme IPv4 devices make up a mere fraction.

The increased range of IP addresses available provides new possibilities for connecting devices to the Internet but also increases complexity in device detection. For a brief moment in time it was possible to scan all hosts in the IPv4 space and obtain a view of their security profile. While it is still possible for IPv4 hosts, the introduction of IPv6 has significantly reduced the possibility to scan the whole IP range. Current Internet scanning tools such as Z-Map are capable of scanning the whole IPv4 address space in approximately 45minutes from a single host machine. There is currently no tool that can produce any result within a viable timeframe for the IPv6 address space (Durumeric, Wustrow & Halderman, 2013). The much larger address space effectively increases the time to scan the whole range to near infinity with current hardware (Caicedo, Joshi & Tuladhar, 2009). On one hand, this is an advantage since it should reduce the effectiveness of worms and other malicious software that use automated means to scan the available networks. On the other hand, this is also a disadvantage since it becomes much harder to effectively detect devices in the IPv6 space. Geolocation technologies will still work, but the accuracy level might drop significantly.

4.4.7 SEARCH ENGINES

A wealth of information is crawled and indexed every day by both commercial and private search engines. The information obtained by these crawlers are made available by many online search engines such as Google[41], Bing[42] and Yahoo[43]. Although online

[40] http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml
[41] http://www.google.com

searches are strongly linked to keywords used, additional filters are normally available to narrow down results returned. Depending on the search provider chosen a collection of specialized keywords exist that allows the search results returned to be filtered by either country, file type or specific web domain. For example, Keywords for the search engines Google, Yahoo and Bing are located at the following URLs:

- Google – https://support.google.com/websearch/answer/136861?hl=en
- Bing – http://msdn.microsoft.com/en-us/library/ff795620.aspx
- Yahoo – https://help.Yahoo.com/kb/search/advanced-search-sln2194.html?impressions=true

Making use of search engine results to find information security flaws is nothing new and a variety of authors have previously published on this topic. A novel security tool dubbed Evilseed that can analyze a known set of malicious URLs and can retrieve similar infected pages based on characteristics was presented by Invernizzi, Comparetti, Benvenuti, Kruegel, Cova and Vigna (2012). Similar in approach is the application PoisonAmplifier, created by Zhang, Yang, Xu and Gu (2012) that utilizes search engines to search for sites with similar keyword or URL structures. The need for technologies such as Evilseed and PoisonAmplifier that enhance search effectiveness is demonstrated by Prieto, Alvarez, López-García and Cacheda (2012). The authors found that simply crawling the web for content is not good enough. Current crawler technology miss information with the best effectiveness obtained by one of the evaluated crawlers coming in at 57.14%. While this reveals more information than it misses, there is still a great deal of room for improvement.

The information security community has also made extensive use of search engines in the past and the approach has popularly become known as Google Dorking. A collection of search terms revealing potentially vulnerable infrastructure is available on ExploitDB[44] under the Google Hacking section. A variety of vulnerabilities and devices can be identified by making use of Google Dork search terminology such as the following:

[42] http://www.bing.com
[43] http://www.Yahoo.com
[44] http://www.exploit-db.com/google-dorks

- **xamppdirpasswd.txt filetype:txt** – This search returns all Google indexed pages that has a vulnerable Xampp installation with the password file open to search engine indexing.
- **intext:"Hikvision" inurl:"login.asp"** – This search returns a variety of Hikvision technology products login portals. Since there a lists available revealing default usernames and passwords, it is a simple avenue of attack.

Search results can often be filtered by criteria such as dates, keywords, URL locations, country or document type containing the indexed information. The potential to retrieve information and limit it specifically in the range required is thus fairly significant.

Taking the previous examples into account it can be considered a simple exercise of building lists of relevant information and retrieving it from available search engines. Unfortunately retrieving information from search engines might seem like a trivial occurrence but there are a multitude of factors contributing to what information is displayed at what time. Factors such as selected search engine, website reputation, malicious activity detected and a significant list most all dictate what information will be displayed at any given time. The results retrieved can also vary widely in a considerably short time span, due to the manner in which search engines index pages. Search Engine Optimization (SEO) is a rapidly growing area of both research and commercial applications and since search engines aim to deliver most relevant content, repeating a search will not always retrieve the same result set. This adds complexity when making use of search engines due to the temporal limitation introduced.

There are limitations to all of the search operators available to the main search engines and unless the user is aware of these limitations, incorrect results can be retrieved. For example, specifying the 'filetype' keyword in a Google search will allow you to retrieve a list of all files with the given extension. Google however, does not index all files and limit their indexing to a few pre-selected file types such as: doc, docx, pdf, csv, xls, xlsm, etc. The search is also case sensitive[45] necessitating the need to check for all case permutations since the extension case is determined by the original application developer. Without the user's awareness of this limitation, it will be assumed that no

[45] https://support.google.com/webmasters/answer/35287?hl=en

files exist for the given search. The Google service also only indexes certain files[46], not everything is indexed and this could lead to missed information.

Another factor to consider is that search engines providers are aware of the potential for malicious use of their platforms and have introduced measures to limit the type of activity allowed. In the case of automated searches, search engine operators attempt to detect automated search queries and then either limit the amount of results returned or, in the case of Google, the re-Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)[47] service will appear. There is also a discrepancies in results obtained when accessing search engines via an API as opposed to doing so through a browser, making reliability harder to achieve.

4.4.8 DATALOSSDB

The DatalossDB[48] project has primary contributions from a variety of privacy regulators, access to public records, news articles and private contributors. At 2014-06-17 a total of three incidents were listed for South Africa on DatalossDB. The results obtained from the DatalossDB service are presented in Table 4-8.

Table 4-8: Dataloss DB[48] recorded results for South Africa on 2014-07-17

Responsible company	Type of data	Incident date	Number of affected records
Direct marketing Association of South Africa	Contact Details, Addresses & ID Numbers	2011-05-30	39000
Diamond Corporation of South Africa	Email addresses	2013-01-29	340
Red Bull South Africa	Administrator Accounts, Username, Passwords & Email addresses	2014-05-21	1714

The 2013 incident in Table 4-8 involving the Diamond Corporation of South Africa, displays only part of the real data breach that occurred on that specific day. The breach involving the Diamond Corporation was part of a much bigger attack dubbed Operation

[46] http://www.google.com/support/enterprise/static/gsa/docs/admin/70/gsa_doc_set/file_formats/file_formats.html
[47] https://www.google.com/recaptcha/intro/index.html
[48] http://datalossdb.org

Sunrise, documented as causing significantly more loss of private information than just 340 records (Swart, Grobler & Irwin, 2013). Table 4-9 provides an overview of all the companies affected by the attack. While the DatalossDB entry is correct it is incomplete and this can be attributed to the manner in which data is obtained. Since the site relies on news articles, personal contributors and submissions to obtain the data, no context is preserved. It is up to the person making the submission to correctly identify the extent of the breach.

Table 4-9: Operation Sunrise records lost summary (Swart et al., 2013)

Company Attackers Claim Information was Obtained From	**Username/ Password Available**	**Password Hashed**	**Encryption Type**	**Data Removed**	**Type of Data Lost**
African Reinsurance Corporation	Yes	Yes	MD5/ Custom	No	Email, Username, Password
Woolworths Holdings Limited	Yes	No	N/A	No	Email, Username, Password, ID, Address, Marriage, Phone, Employment history
South African Diamond Corporation	No	N/A	N/A	No	Email
African Mining	Yes	Yes	N/A	No	Email, Title, Position, Username, Password
BEE Network	Yes	Yes	MD5 / Custom	No	Email, Title, Username, Password, Address, Financial
Allied Technology International	Yes	Yes	MySQL / MD5	No	Email, Username, Password
I Llovo Boulevard (I llovo Corporation)	Yes	Yes	MySQL / MD5	No	Email, Username, Password
Genesis Insurance Brokers	Yes	Partial	MD5 / MD4	No	Email, Username, Password, Phone, Correspondence
Omni ID Company Part	Yes	No	N/A	No	Email, Username, Password, Phone, Correspondence, Address
Ornico Marketing	Yes	No	N/A	No	Email, Username, Password, Phone, Address
Moolmans Africa Mining Corporation	Yes	Partial	Custom	No	Email, Username, Password
Angola's National Diamond Corporation	No	N/A	N/A	No	Email
Angola's Oil field industries	No	N/A	N/A	No	Database Structure
South African Express Petroleum	Yes	Yes	SHA-1 / MySQL5	No	Email, Username, Password
State University Part	Yes	Partial	MD5 / MD4 / MySQL	No	Email, Username, Password, Phone,

Company Attackers Claim Information was Obtained From	Username/ Password Available	Password Hashed	Encryption Type	Data Removed	Type of Data Lost
			160 bit		Address, Correspondence
Westcol College	Yes	Yes	MD5 / MD4	No	Email, Username
The Inc Company	Yes	Yes	SHA-256 / Haval-256	No	Email, Username, Password, Phones
Sasol Corporation	Yes	Yes	MD5 / MD4	No	Email, Username, Password
Kenyan Business Directory	No	N/A	N/A	No	N/A
Algerian Government website	Yes	Yes	MD5 / MD4	No	Username, Password
PressOffice linked to BidOrBuy, South Africa's largest online store	No	N/A	N/A	No	Names, Phones
FreightForwarders	Yes	No	N/A	No	Email, Username, Password, Phone, Correspondence, Address
PostNet Internet Services	Yes	Partial (NedCare)	MD5	No	Email, Username, Password, Phone, Correspondence, Address

In total the operation Sunrise incident leaked the following amount of information:

- 5107 identifiable physical addresses.
- 18004 telephone numbers.
- 11703 unique username and password combinations.
- 19849 South African ID numbers.
- 1641 tertiary and secondary school education details.
- 45721 email addresses.
- 1632 marriage statuses

While the hackers targeted South African companies, the data leaked contained information relating to individuals and physical locations both nationally and internationally. The leaked locations are presented in Figure 4-6.

Figure 4-6: Physical locations extracted from the data leak (Swart et al., 2013)

From the example above it is clear that while DatalossDB provides an excellent aggregate overview of the data loss landscape where there are central reporting authorities, the true extent of loss is potentially much greater.

4.5 METADATA DATASETS

In contrast with object datasets (discussed in Section 4.4), metadata datasets provide information regarding the properties of the objects located in the Internet domain. While the datasets might contain information such as IP addresses, names or some form of unique identification, the focus is typically to describe the object in more detail. The unique identifiers listed in the metadata dataset is merely to provide a link back to the original object as described in the data sources object in Section 4.4.

4.5.1 HACKERWEB

Hackerweb[49] is an aggregator that serves a variety of content from a collection of news and community sources. The data source was previously used by Bhatia, Hussaini, Navalakha and Zhou (2014) to examine questions such as: *When hackers are the most active on forums?* or *What is the most frequently asked questions?* The content of the site is rarely of such a nature that it can directly be used to exploit a system in the wild. The information contained is of great interest to the typical person interested in information security. Information such as typical operational hours for attackers can benefit defenders in their evaluation of situations occurring during the day. New topics and trends that affect security is also of prime importance here since the forums section of the site provides a ranking score for contributors. Obtaining insight into the type of

[49] http://cheeaun.github.io/hackerweb

questions and news most consumed by various levels of potential attackers can also serve to enhance the operational understanding of the defending team. The information obtained from this data source while useful does not directly contribute to the understanding of national infrastructure and are therefore not included for the experimental system.

4.5.2 GEOLOCATION

Geolocation technology provides the ability to point to a latitude and longitude where a specific device is thought to be located. The use of such technology is vast and ranges from traditional asset management to more complex tasks such as obtaining attribution from a country after a cyber incident. Typically, geolocation on the Internet is achieved by examining the IP address of a system and then performing lookups to determine the nationality of the registered IP. Obtaining higher resolution geolocation is possible by performing queries to specialized databases, such as those presented by MaxMind, Skyhook and several others, that contain information regarding the potential state, suburb and in a variety of instances, even the street address of a specific device. It has previously been argued that the use of third party libraries and client support are not an exclusive requirement and that using the known average latency of network connections can achieve up to a 690 meter accuracy level (Y. Wang, Burgener, Flores, Kuzmanovic & Huang, 2011). These types of solutions are all in instances where counting on the support of the device operator is not involved. If device operator support is available a variety of web services are available to obtain significant accuracy.

A variety of researchers have discussed accuracy of geolocation services. Geolocation from commercial datasets was evaluated by Poese, Uhlig, Kaafar, Donnet, and Gueye (2011) and the researchers found that geolocation was accurate 76% of the time for China. The work considered five geo-libraries: HostIP, IP2Location, InfoDB, Maxmind and Software77. The overall conclusion was that the higher the resolution expected of the service the lower the accuracy. To simply determine the country of origin the geo-library services achieved a 96% and 98% accuracy. As soon as the location of the IP address needs to be pinpointed to a street block, apartment building or physical location the accuracy was nearly never correct. The type of network that the device is located on also plays a significant role in accuracy. For example, when the device is located on a cellular network, geolocation of the device might significantly differ from the device's real location.

Extending the research performed on geolocation, researchers found that with enough data from the libraries, it becomes possible to infer the topology of ISPs serving a specific geolocated area under investigation (G. Wang, Zhang, Qiu & Zeng, 2011). Another proposal to improve accuracy was to crawl the Internet-based Point of Presence locations of ISPs. Other approaches documented include:

- Delay based methods
    - Constraint based geolocation
    - Speed of Internet
- Topology based geolocation
- Web parsing (Taylor, Devlin & Curran, 2012)

With enough continuation of research into this type of work, effective geolocation techniques will be able to pinpoint the location of devices. Greater accuracy will improve situational awareness and this could be of significant use to CERTs and other defending institutions as documented in Chapter 3. A brief examination of the various prominent geolocation technology services is presented in the next sub-sections.

4.5.2.1 SKYHOOK

The Skyhook service[50] provides a variety of services that allow real-time location of devices based on their IP addresses or proximity to recorded WiFi and mobile telecommunication access points. A variety of methods to interact with the dataset are available, including an API or a bulk download that is updated monthly as part of an ongoing valid account. Pricing of the service depends on the amount of data required and can only be obtained from the Skyhook sales department. Coverage of the Skyhook database for South Africa is not as extensive as it is in the USA or European regions but as depicted in Figure 4-7, the major metropolitan areas does have significant coverage.

Previous research has shown the service to be accurate to approximately 10 meters with client interaction (Vratonjic, Huguenin, Bindschaedler & Hubaux, 2014). Accuracy drops when a static lookup is performed but Skyhook provides additional data when a query is performed to allow the user to gauge how accurate the data might be. The static lookup fields returned indicate estimated confidence relating to the country, state and city of the selected IP address in Figure 4-8. A key field that can also be considered potentially valuable is the field indicating the type of the IP address queried.

[50] *http://*www.skyhookwireless.com

Figure 4-7: Skyhook[50] coverage on 2014-06-08

In the example provided in Figure 4-8 the type is FIXED and this provides assurance that the IP address is static in location and not expected to be found at other geographic locations. Should a device with a vulnerability thus be detected and located via a service such as Skyhook, priority can be assigned to FIXED devices since they should be easier to track down. Devices that do not have static IP addresses only retain the address for a certain amount of time and once the IP is renewed, the geolocation service would first have to detect the newly assigned IP address, then correlate it with a potentially previously identified device to provide reliable geolocation services.


```
{
  "data" : {
    "location" : {
      "type" : "FIXED",
      "latitude" : -25.747129440307617,
      "longitude" : 28.29949951171875,
      "hpe" : 50000.0
    },
    "ip" : "146.64.8.10",
    "civic" : {
      "state" : "Gauteng",
      "country" : "South Africa",
      "countryProb" : 0.99,
      "countryIso" : "ZA",
      "stateProb" : 0.99,
      "stateIso" : "GT",
      "city" : "Pretoria",
      "cityProb" : 0.99
    }
  }
}
```


Figure 4-8: Skyhook API return result

In addition to the location services provided, Skyhook also allows for community participation to improve the results obtained from the current databases. Should any errors be detected, a submission page is available for users to submit precise co-ordinates.

4.5.2.2 MAXMIND

Maxmind[51] provides both a free and commercial version of their IP address to geolocation library. The two services differ in the level of accuracy they provide and the frequency of updates to the database provided, with the paid version being the most frequently updated and more precise. The service provides multiple ways to access the dataset via either an online API or an offline database containing the required information. Accuracy between various countries are not similar due to the differing legislation, regulatory requirements and the manner in which ISPs choose to setup infrastructure. Given these differences Maxmind provides accuracy levels, available in Figure 4-9, and states that the error ratio drops 1.5% for each month that the database is not updated.

Country	Correctly resolved within forty kilometers	Incorrectly resolved	City is unknown
South Africa	71%	24%	5%
Spain	80%	15%	5%
Sri Lanka	41%	8%	51%
Sweden	67%	14%	19%
Switzerland	72%	10%	18%
Taiwan	86%	13%	1%
Thailand	66%	20%	14%
Trinidad and Tobago	88%	5%	7%

Figure 4-9: Maxmind[51] accuracy level internationally on 2014-06-16

Previous research making use of the Maxmind service include works that measure both the service's accuracy levels (Poese et al., 2011) or works implemented using the service. An example of the latter is a visualization of spam generated on a geolocated system (Muallem, Shetty & Hargrove, 2013). The API call is available in the form of simple JavaScript script that needs to be included and called in the manner shown as Figure 4-10.

[51] https://www.maxmind.com

```
<script type="text/javascript" src="//js.maxmind.com/js/apis/geoip2/v2.0/geoip2.js"></script
>

<script type="text/javascript">

var onSuccess = function(location){
    alert(
        "Lookup successful:\n\n"
        + JSON.stringify(location, undefined, 4)
    );
};

var onError = function(error){
    alert(
        "Error:\n\n"
        + JSON.stringify(error, undefined, 4)
    );
};

geoip2.city(onSuccess, onError);

</script>
```

Figure 4-10: Maxmind[51] JavaScript API call structure

Should the call be successful a JSON structure (not unlike the Skyhook web service structure as shown in Figure 4-8) will be returned to the user. The most significant difference being the support for multiple languages provided by Maxmind, resulting in a larger object.

During the examination of the Maxmind GeoLite database used in the experiment, a detailed matching to the IP addresses published for South Africa by AFRINIC was performed. The results of the evaluation is available in Table 4-10 for IPv4 addresses and the IPv6 evaluation is available in Table 4-11.

From the data listed in Table 4-10, it would seem that the open source database Geolite from Maxmind provides coverage for the South African IPv4 space at approximately 50.58%. The data presented in Table 4-10 in three columns, where the first column contains the first octet of the IP addresses assigned by AFRINIC to the South African domain. The second column performed a summary count of the number of times the first octet occurred in the South African assigned range from AFRINIC. Column three records the number of IP ranges found to be missing, once matching between the assigned AFRINIC ranges and the available Maxmind GeoLite IP ranges were performed. Data listed in Table 4-11 follows the same pattern for the IPv6 ranges assigned to South Africa.

Table 4-10: Evaluation of Maxmind Geolite library IPv4 addresses assigned to South Africa on 2014-08-28

IPv4 Address first octet assigned by AFRINIC	Frequency of first octet assigned to South Africa	Maxmind Geolite not recognized ranges
41	149	24
66	2	0
69	1	0
81	1	1
105	11	1
137	4	1
139	1	0
143	2	0
146	6	1
147	1	0
152	7	4
154	59	14
155	10	7
156	1	0
160	11	3
163	9	6
164	3	0
165	10	0
166	1	0
168	11	1
169	7	2
192	207	192
196	409	174
197	51	6
198	132	123
200	1	0
204	3	1
205	1	1
206	1	1
209	2	0
213	2	2
216	1	0
Totals	1117	565

Table 4-11: Evaluation of Maxmind Geolite library IPv6 addresses assigned to South Africa on 2014-08-28

IPv6 Address first octet assigned by AFRINIC	Frequency of address assigned to South Africa	Maxmind Geolite not recognized ranges
2001	43	6
2c0e	1	0
2c0f	73	4
Totals	117	10

The IPv6 ranges have a much higher representation in the GeoLite library and indicates a 91.4% coverage for the South African domain. No reason for the discrepancy in accuracy could be obtained and it should be noted that the database evaluated is the free version. A commercial version is available that claims a much higher accuracy.

4.5.2.3 HostIP

HostIP[52] is operated by a non-commercial company and is the result of work performed by a community of contributors. The database is downloadable free of charge and the community recommends the use of the Maxmind geolocation service should a more reliable service be required. An API is also available and similar in operation to the service provided by the Maxmind database.

While the service was previously regularly updated, the last downloadable update is dated the 2013-02-13. No published accuracy statistics could be located.

4.5.2.4 IP2Location

IP2Location[53] is a geolocation service provider that also provides information such as the elevation and weather available at the detected address. The service provides limited free lookups to a pre-selected range of IP addresses in the form of downloadable databases. Accuracy is made available by the vendor and displayed in Figure 4-11. Accuracy degradation is estimated between 1% and 5% per month.

Country Code	Country Name	Total IP Address	City Coverage	Accuracy (<50 miles)
VN	VIET NAM	15,568,158	99.26%	83.54%
VU	VANUATU	21,010	99.99%	82.96%
WF	WALLIS AND FUTUNA	4,365	99.99%	93.57%
WS	SAMOA	23,844	99.99%	68.01%
YE	YEMEN	74,999	91.15%	66.25%
YT	MAYOTTE	11,034	99.99%	74.07%
ZA	SOUTH AFRICA	23,620,162	98.65%	72.29%
ZM	ZAMBIA	325,971	97.99%	74.96%
ZW	ZIMBABWE	126,057	94.52%	75.98%

Figure 4-11: Sample of IP2Location[53] claimed accuracy on 2014-06-16

[52] http://www.hostip.info
[53] http://www.ip2location.com

The online API method of operation is similar to both the MaxMind and Skyhook services that returns an object containing the information obtained from the lookup. The IP2Location service offers a variety of free API implementations in a variety of languages such as Ruby, C and Pascal. A commercial version of the API is alternatively available for programming languages such as C#, JAVA or ASP .NET.

4.5.2.5 INFODB

The InfoDB[54] service is powered by the IP2Location service and does not offer any value added service over the original provider. As such, it is included in the list but will not be discussed in greater detail. Similar API and downloadable databases as the IP2Location service is available to the user.

4.5.2.6 SOFTWARE77

The geolocation service provided by Software77[55] reports back only the country of the provided IP address. The data is available via an online API submission request similar to the Maxmind and Skyhook interfaces. Alternatively, the data can be downloaded in a database file format for offline use.

An additional service provided lists all the IP ranges that is allocated to a country via the registrar. While this is not strictly part of geolocation, it is a useful reference when comparing allocated IP addresses to various countries.

4.5.3 GEO-SPATIAL DATA

Currently observed cyber attacks have not yet made use of geo-spatial data, rather relying on geolocation in the cyber domain. The possibility of making use of this type of data should however not be discredited (Baker, Lachman, Frelinger, O'Connell & Hou, 2004). Physical security is an integral part of the security chain and damage is almost a certainty when physical breach is possible due to the increased number of potential attacks (Hammer, 2006). The lines between physical and cyber are increasingly dissolving with the integration of networked electronics in physical security devices. This has resulted in virtually all physical electronic authentication technology to suffer some form of information security vulnerability in the past decade.

As geolocation accuracy increases the potential to overlay Geographic Information System (GIS) data and obtain a clearer picture of what systems are present at a specific

[54] http://www.ipinfodb.com
[55] http://software77.net

location might not be farfetched. It is already possible to determine the IP address of a given organization and perform a full scan on their infrastructure exposed to the Internet. By plotting the obtained scan data to a map, it can potentially allow attackers to identify access control systems such as perimeter defenses among the scan results.

4.5.4 CUSTOM DICTIONARIES

Many communities have their own manner of communicating with their peers and the information security community is no different. Hackers specifically have traditionally used a form of writing known as Leet speak where vowels are typically dropped and digits are inserted into the word where it is required. This allows for faster typing and also is often hard for a non-versed person to translate easily. Just as Natural Language Processing plays an important role in topic modeling, the detection of Leet speak in potentially unexpected places can be an indicator of hacker activity.

Since Leet speak is not an official language, finding word lists or dictionaries of available words is not always possible. While there are a variety of dictionaries available, not one of them is considered as complete. To generate the Leet speak database used in this experiment, both relatively small English and Afrikaans dictionaries were downloaded from MD5This[56]. These dictionaries contain basic words in both English and Afrikaans that are commonly used in the South African context. To transform the downloaded dictionaries into Leet speak dictionaries, the password cracking utility HashCat[57] was used. HashCat has the ability to accept rules on how dictionary words should be transformed and as of 2014-04-14 two Leet speak rules are available. One version is a relatively simple rule to replace characters such as 'S' with '$' to obtain a result such as "Acce$$" versus the original "Access". However this is a single example, and there are many permutations required to generate a comprehensive dictionary. Since Leet speak is not an official language, characters substitution and replacement is performed by the individual at will. While the simple rule set is quite fast, it will not generate all permutations of a word. For example,

- P455w0rd - Generated
- P@$$w0rd - Not generated
- P4$$w0rd - Not generated
- P@55w0rd - Not generated

[56] http://www.md5this.com/tools/wordlists.html
[57] http://hashcat.net

The more advanced version named "Ninja-leetspeak.rule" included in the default HashCat installation will generate a larger number of permutations such as:

- Pa$$word
- p455w0rd
- p455word
- p4ssw0rd
- p4ssword
- pa55w0rd
- pa55word
- passw0rd

Due to the increased processing required, the generation of the comprehensive file is also significantly slower and makes increased use of disk space. It should be noted that rules can be customized according to own requirements and a whole rule scripting language has been implemented by the HashCat creators.

4.5.5 SENDERBASE

Senderbase[58] is a project funded and operated by the CISCO corporation and the data contained reflects the email traffic that CISCO has access to worldwide. The project aims to track the global volume of email flowing through their networks to determine the amount of spam that each country is responsible for. Figure 4-12 presents an overview of the data that Senderbase have in their possession on a geolocated map.

From Figure 4-12 it is clear that there is hardly a nation on earth that does not contribute to the volume of spam flowing through the Internet infrastructure. Spam is a serious problem and while it is estimated that only 0.25% of all spam messages sent are clicked on, it still costs the world economy approximately $20 billion (Rao & Reiley, 2012). The African continent typically sends less spam than other continents, mainly due to the comparatively low number of people connected to the Internet in Africa (Kyobe et al., 2012). However, as broadband penetration increases, so will cyber crime activity. South Africa is already the top contributor to spam on the continent.

[58] http://www.senderbase.org

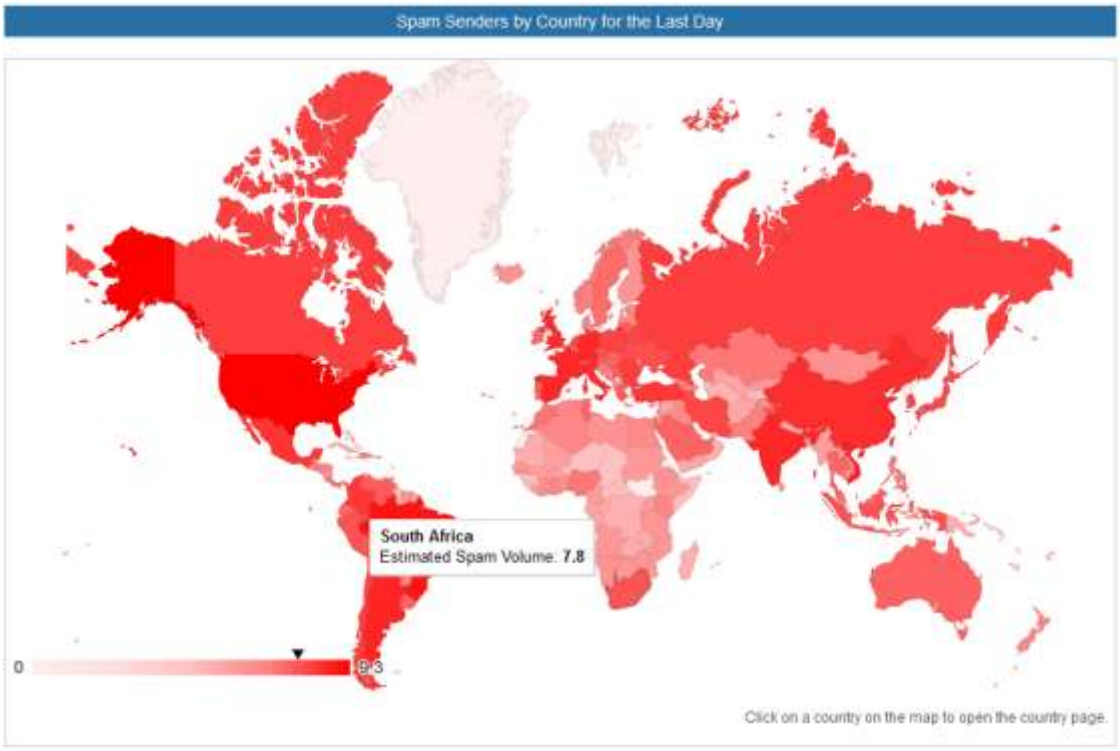

Figure 4-12: South Africa volume of spam on 2014-06-21 compared internationally[58]

4.5.6 REALTIME ATTACK TRACKERS

A variety of entities have invested in real time visualization to convey the volume and types of attacks they have access to. Corporations that offer some sort of visualization include Norse[59], Kaspersky[60], Akamai[61] and Arbor[62]. Although most visualizations make use of geolocations, the data presented on the locations are often significantly different due to the type of information available to the corporation. For example, the Norse corporation chose to visualize its system based on the type of network protocol that was used in an attack and this allows the user to hover over a location and view the types of protocols used to attack a site. The visualization is depicted on a two dimensional map that does not have the functionality to zoom or pan left or right with a variety of legends to explain the information presented. The Norse system is depicted in Figure 4-13 and illustrates how hovering over a selected node can show a history of attacks, location and convey information regarding the type of protocol used. In the screenshot, South Africa cannot claim to have no participation in attacks since at least three instances were recorded in the time period during which the system was evaluated.

[59] http://map.ipviking.com

[60] http://cybermap.kaspersky.com

[61] http://www.akamai.com/html/technology/dataviz1.html

[62] http://www.digitalattackmap.com

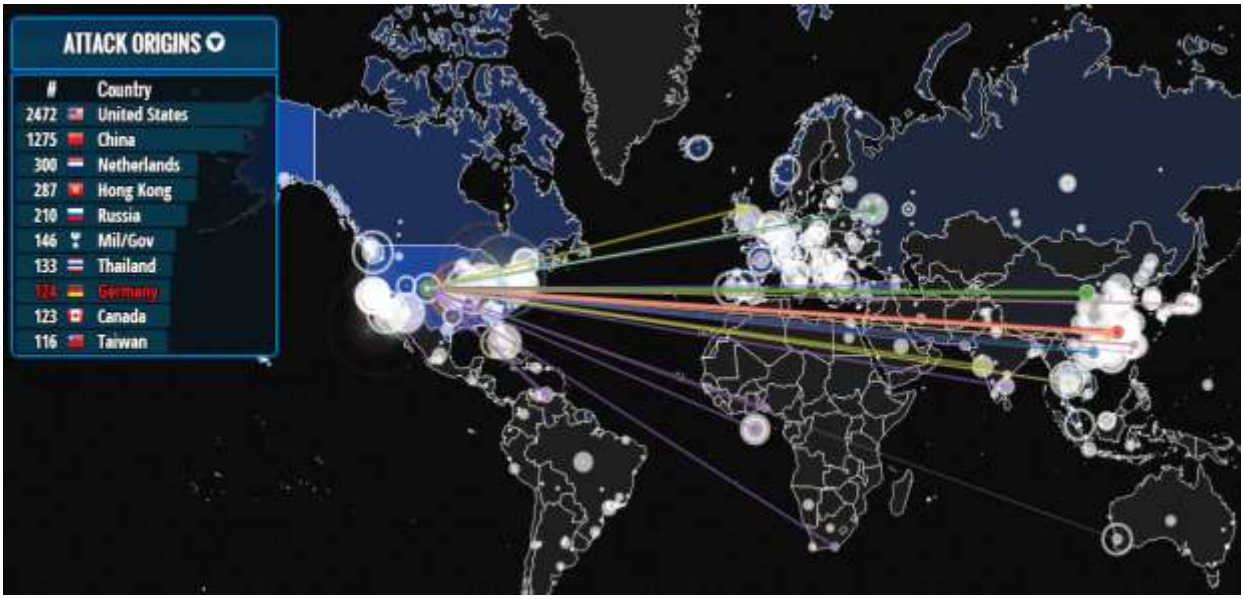

Figure 4-13: Norse corporation IP Viking map[59] on 2014-07-02

The previously discussed system from the Norse corporation conveyed information regarding the activities that occurred on networks under their control. This is similar to the visualization from the Akamai and Arbor networks, although it should be noted that each chose different visualization techniques and data in their respective systems. A visualization system from Kaspersky provides feedback regarding networks under their control and also conveys information from the systems that they have deployed at client networks worldwide.

The distinction in data sources can be significant: all of the systems described above obtain data from networks under their own control except for Kaspersky. Kaspersky obtains data from a variety of individuals, organizations and governments who make use of their products. This allows for a far greater aggregate view of the locations where attacks occur and a finer granularity on reporting what types of attacks occur. A limited view of the Kaspersky system is depicted in Figure 4-14, zoomed in on the South African region. According to Kaspersky on 2014-06-28, South Africa was the 8th most infected country in the world when clicking on the country on the interactive map. The data presented in the system is not described as real-time and the ranking fluctuates depending on the activity measured in a country.

Figure 4-14: Kaspersky corporation attack map[60] on 2014-07-10

The Kaspersky system, unlike the Norse system, ignores the Internet protocol used in the attack and instead focuses on the type of attack detected. Another interesting aspect of the system was that where possible both the origin and the destination IP address are visualized by making use of a color coded beam spanning the source and destination IP addresses. In not one of the systems investigated was the data available for either download or access via a free or paid API.

4.5.7 VULNERABILITY DATABASES

Most vulnerabilities are reported via a CVE number, although it should be noted that this is not always the case and that other numbering schemas exist. This is due to the fact that vulnerability databases are operated by a variety of organizations and the manner in which they classify vulnerabilities differ. CVE is one of the most popular vulnerability descriptors and was created as a standard schema implemented by the MITRE[63] organization to facilitate the sharing of information about information security vulnerabilities. The schema has attracted a significant following with a variety of

[63] http://cve.mitre.org

international software and hardware vendors participating in reporting flaws in their software. When a vulnerability is reported with a CVE description, the numbering authority assigns a vulnerability number allowing multiple entities to collaborate by referencing a common number. The CVE numbering authority consists of a few key industry vendors but MITRE remains the prime numbering authority.

A CVE is typically published along with additional information such as a Common Vulnerability Scoring System (CVSS) score that is calculated by following a set of predetermined criteria. CVSS criteria including the type of access required for the exploit to function and what the impact of the exploit is, all contribute to a set of scores. The obtained scores provide a quantifiable way for a variety of groups to interact and judge the potential severity the CVE number might have on their organization. While it is possible to calculate the score manually a variety of online calculators are available to ease the task. One such is example is the CVSS calculator[64] created by the CISCO corporation that provides entities with the ability calculate a CVE score related to their organization. A collection of CVE reports is typically published in the Common Vulnerability Reporting Framework (CVRP) format that is maintained by the Industry Consortium for Advancement of Security on the Internet[65]. CVRF reports are published by industry vendors and contain as much as possible information regarding the CVE.

Care should be taken when a vulnerability is disclosed not to simply accept the number as the amount of vulnerabilities reported for the year. A number of vendors make use of the CVE system by pre-allocating a number of vulnerabilities to their organization. Thus, if a new vulnerability is discovered by an entity external to the organization, the next number available will not be the actual number of CVEs for the year allocated but the next number after the block booking. The CVE schema is updated constantly with one of the most recent changes being the lengthening of the field responsible for the number of vulnerabilities reported for a year. Instead of the traditional field that was defined as four digits, it was now amended to be expandable to as many digits as is required by the CVE numbering authorities. This was done to allow for the reporting of vulnerabilities larger than nine thousand nine hundred and ninety nine that was previously possible.

[64] https://intellishield.cisco.com/security/alertmanager/cvss
[65] http://www.icasi.org/cvrf

The National Vulnerability Database[66] (NVD) on 2014-06-23 contained 46374 entries spanning over a decade while the Open Source Vulnerability Database[67] (OSVDB) claims 106877 vulnerabilities documented. The vulnerabilities in the NVD are presented in a structured format with information such as CVE name, description of the flaw, severity of impact score and ease of exploitation score. There is no official repository of all known vulnerabilities due to the unstructured nature of the Internet. Security researchers finding a vulnerability can choose to report the vulnerability to whomever they want. If it is never submitted to a vulnerability database to allocate it a CVE number, the vulnerability might not be listed in the NVD, but could be uploaded to another vulnerability database such as OSVDB. While the NVD is one of the biggest databases available, it might never reach the official updates due to the previously mentioned unstructured nature of information security. Another collection of available exploit is hosted at ExploitDB[68] with one of the main differentiators between NVD, OSVDB and ExploitDB being that the latter also provides Proof of Concept (POC) source code and instructions. ExploitDB also attempts to host the application that the vulnerability was detected on for experimentation purposes. Hosting old applications might seem like a trivial feature at first but due to the way the Internet and technology continuously progresses forward, obtaining the source or executable for a POC can be extremely difficult. As a result, having the proof of concept code is of little use if a vulnerable application is not available to examine the manner in which the exploit functioned.

Vulnerability disclosures and statistics contained in vulnerability databases are often used in reports to present graphs and statistics regarding information security. There is however a significant problem with this type of approach due to the multiple types of bias present in vulnerability databases (Christey & Marion, 2013). As a result of these types of bias available these databases should by no means be considered as perfectly reliable sources to generate statistics from. In Table 4-12 the various types of bias are summarized based on the actor involved in the reporting of the vulnerability.

[66] http://nvd.nist.gov
[67] http://osvdb.org
[68] http://www.exploit-db.com

Table 4-12: Bias in vulnerability databases (Christey & Marion, 2013)

	Researchers	**Vendors**	**VDBs**
Selection bias	Choose particular products or vulnerability types to research	Conduct internal research based on internal priorities; work with external researchers	Monitor certain disclosure sources
Publication bias	Might publish only for high-profile products; avoid low-risk and "lame" vulnerability types	Only publish patched, high-severity issues for currently supported products & versions	Only publish "verified" issues of a certain severity for "supported" products
Abstraction bias	Release many advisories for one core issue, boosting counts	Combine many vulnerability into the same advisory for sysadmin convenience	Use the level that is best for the intended audience
Measurement bias	Over-estimates severity, or does not validate findings	Under-estimates severity or uses generic vulnerability terms	Misinterprets external disclosures

Not all vulnerability databases focus on the same vulnerabilities and in some instances, there are projects created to find hosts available on the Internet with a documented vulnerability. The Un1c0rn[69] project is one such example that does not go into detail regarding the vulnerabilities themselves but rather attempts to focus on finding hosts available on the Internet with the previously detected vulnerabilities. The vulnerabilities are typically listed by their detected IP address and domain name along with the results of the vulnerability found on the website. In some instances, the information is only available as a preview and for full disclosure payment is required. While South Africa is typically not as comprehensively indexed as the United States or European countries, results for a variety of vulnerable servers are available. A search on project Un1c0rn reveals 85 hosts with the keyword "co.za" in their headers vulnerable to a variety of disclosed items in Figure 4-15.

[69] http://un1c0rn.net/?module=dump&action=list

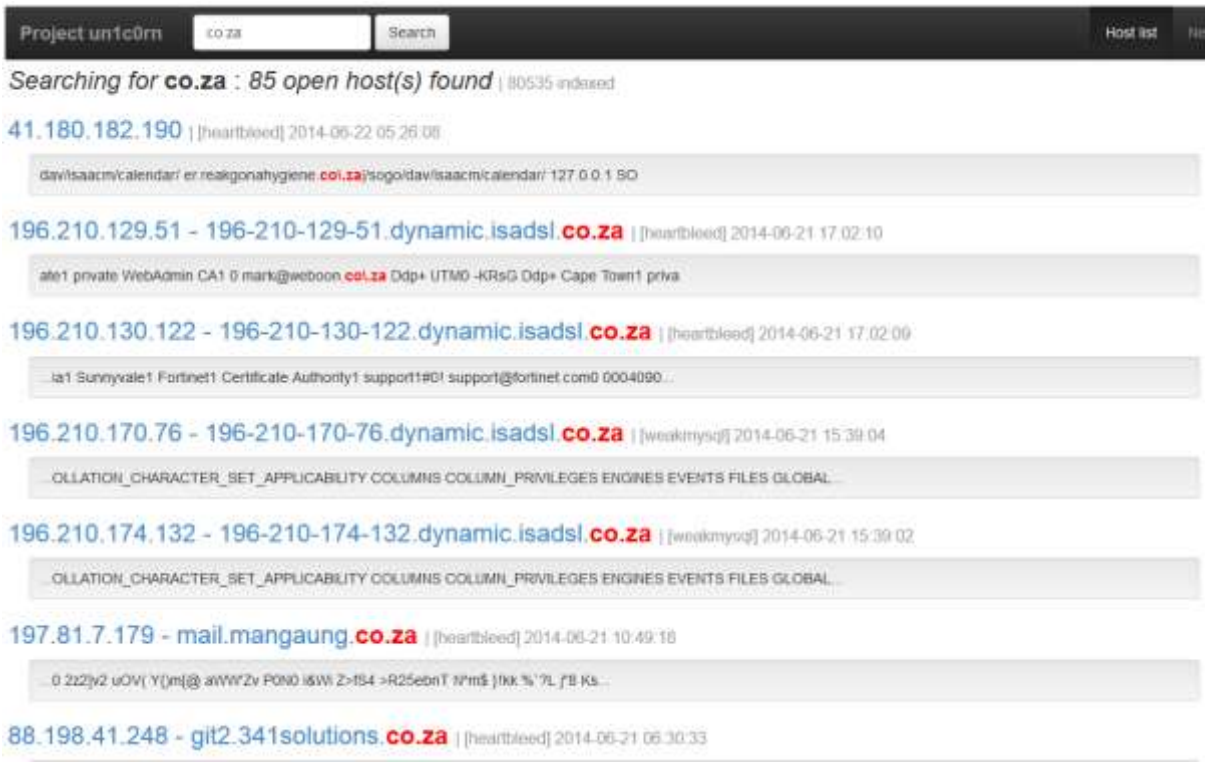

Figure 4-15: Project Un1c0rn results for the co.za namespace on 2014-06-22

What makes the Heartbleed bug noteworthy enough to set up vulnerability watch lists (as shown in Figure 4-15), is the widespread availability of the bug and the potential to gain access to sensitive information. The Heartbleed bug was discovered in the OpenSSL library in early 2014 and assigned CVE-2014-0160 (Gujrathi, 2014). The bug relies on a programming error where the heartbeat function of OpenSSL may be exploited to request more information than what is strictly required. This allows an attacker to request a potentially large chunk of data that is stored in memory. While the information retrieved is arbitrary, several documented examples exist where sensitive information such as security certificates, usernames and passwords and a variety of information has been obtained.

Examining the results retrieved from the Un1c0rn project revealed an interesting set of results regarding the infrastructure in South Africa. Not only were a variety of dynamic IP addresses vulnerable, but a whole range of dedicated IP addresses were also listed in the result set. From the given hostnames, domains can be inferred and a significant number of the hosts were from companies listed on the South African stock exchange. While this is to be expected from the vulnerabilities reported by the service, more analysis is required since the data might show that Small and Medium Enterprises require just as much information security assistance and information as bigger organizations.

4.5.8 HONEYPOTS

Honeypots are applications placed on a network that simulate a real infrastructure device such as a router or PC. Since the honeypot is not a real device, it provides an opportunity to examine the attack methodology used by malicious entities without potentially compromising real devices. Typically logging and various levels of emulation is available to make the system seem as real as possible.

Project Honeypot[70] has at current count more than 50 active entries for the South African IP space with unique active occurrences going back as far as 2007. The site has data available relating to the South African landscape as far back as 2004 and all of this is available on request. Data offered includes the IP address of the originating attack, the type of offence committed, the total times that the specific IP has been detected in the dataset and the last time the IP address performed an attack on a honeypot in the network. Offence abbreviations are as follows:

- Spam servers – A server that is detected to send out spam email.
- Dictionary attacker – Makes use of a mail server to randomly build up commonly used names via a dictionary, sending a mail to random address and check if it has been delivered. This is in aid of building a list of valid email addresses to use in future spam campaigns.
- Web host – A bad web host is defined as a host that is used to host malicious applications. While possibly started with a legitimate purpose, it is now host to malware.
- Harvesters – Used to crawl the Internet in search of e-mail addresses to be used by spammers in future spam campaigns
- Rule breakers – IP addresses that performed scans or had an active interest in IP addresses associated with a honeypot that should never have legitimate traffic.
- Comment spammers – Post links to sites to illegally increase their search rankings on search engines. Alternatively, the links can point so servers loaded with malware to further grow the compromised botnet army.
- Search engines – Fake search engines deployed to route visitors to destinations that fraudsters are trying to improve in search engine rankings or for advertising revenue.

[70] http://www.projecthoneypot.org

The information listed in Table 4-13 shows the South African IP addresses that have attempted to contact the honeypots under the control of Project Honeypot. Since Project Honeypot offers no real services, the assumption is, that it should never be contacted by any non-malicious device. Any such communication is classified according to pre-determined categories depending on the behavior observed explained in the section above.

Table 4-13: Project Honeypot's top 50 active South African IP addresses on 2014-06-16

IP	Offence[71]	Total	First Seen	Last Seen
196.28.101.191	SD	43	2007-06-12	2014-06-16
196.28.101.192	S	67	2007-08-06	2014-06-16
196.28.80.29	SD	45	2010-06-01	2014-06-16
196.28.80.24	S	28	2010-08-04	2014-06-15
196.46.176.253	SDW	16	2010-10-12	2014-06-17
41.193.4.183	S	10	2011-01-12	2014-06-16
196.210.128.181	S	11	2011-03-09	2014-06-16
196.210.140.210	D	55	2011-04-20	2014-06-17
196.220.38.66	W	6	2012-10-17	2014-06-16
41.242.112.10	SC	84	2013-12-17	2014-06-17
41.207.229.130	SD	93	2014-02-16	2014-06-16
41.203.16.129	S	18	2014-02-26	2014-06-17
196.33.209.118	SD	20	2014-03-25	2014-06-17
196.28.125.34	SD	51	2014-04-08	2014-06-16
41.183.7.6	SD	27	2014-05-08	2014-06-15
41.242.115.22	S	5	2014-05-13	2014-06-14
196.210.167.103	D	5	2014-06-04	2014-06-17
196.46.182.130	D	3	2014-06-04	2014-06-17
41.183.48.32	D	3	2014-06-04	2014-06-16
165.165.233.206	SD	5	2014-06-05	2014-06-17
196.209.217.14	S	4	2014-06-05	2014-06-17
196.215.171.52	-	2	2014-06-09	2014-06-17
41.160.232.218	C	11	2014-06-09	2014-06-15
196.215.19.12	S	3	2014-06-10	2014-06-17
196.214.136.50	S	3	2014-06-13	2014-06-13

[71] S = Spammer, D = Dictionary attacker, W = Bad web host, - = Not classified but suspicious

IP	Offence[71]	Total	First Seen	Last Seen
196.214.90.146	-	2	2014-06-13	2014-06-16
41.185.13.53	W	9	2014-06-13	2014-06-17
41.150.146.224	-	1	2014-06-14	2014-06-14
41.160.80.132	C	10	2014-06-14	2014-06-14
196.15.254.90	D	10	2014-06-15	2014-06-15
196.215.109.102	D	2	2014-06-15	2014-06-15
196.34.89.21	-	1	2014-06-15	2014-06-15
196.41.123.237	-	1	2014-06-15	2014-06-15
196.210.125.147	-	1	2014-06-16	2014-06-16
196.210.179.250	S	5	2014-06-16	2014-06-17
196.211.88.62	-	1	2014-06-16	2014-06-16
196.215.72.59	-	1	2014-06-16	2014-06-16
196.34.234.61	-	1	2014-06-16	2014-06-16
196.41.110.138	-	1	2014-06-16	2014-06-16
41.151.165.15	D	34	2014-06-16	2014-06-16
41.185.12.55	W	2	2014-06-16	2014-06-16
165.145.136.167	SD	7	2014-06-17	2014-06-17
165.145.45.133	S	2	2014-06-17	2014-06-17
196.10.252.29	-	1	2014-06-17	2014-06-17
196.210.102.62	D	61	2014-06-17	2014-06-17
196.210.198.79	-	1	2014-06-17	2014-06-17
196.215.43.113	S	3	2014-06-17	2014-06-17
209.203.50.116	-	1	2014-06-17	2014-06-17
41.150.113.217	-	1	2014-06-17	2014-06-17
41.177.108.33	-	1	2014-06-17	2014-06-17

With a list as comprehensive as in Table 4-13, it should be fairly easy to maintain security in a national environment. The list contains all the required information to at least narrow down the search for the owner and there is evidence that malicious activity in some form has been performed from the specified IP address. Unfortunately, due to the way in which the Internet is structured, it is not always possible to place blame with much confidence without extensive further research.

Consider the very first IP address in the list, 196.28.101.191, that has been active since 2007 and has been detected 43 times up to now. It is possible to obtain proof of the types of messages sent from the IP address and even to see associated Harvesters spanning international borders in Figure 4-16. This all builds up the confidence that the host under examination is indeed a malicious host and requires a security audit and potentially malware software removal.

Figure 4-16: Spam headers received from 196.28.101.191 detected by project Honeypot[70] on 2014-06-16

Now consider that once a more detailed investigation into the server with IP address 196.28.101.191 is performed, the server is revealed to be part of the SMTP servers used by the large South African ISP Mweb[72]. Considering how the architecture of the Internet works and that a large number of hosts are most probably making use of the SMTP server for their mail needs, it becomes clear that the server is in all probability not the actual offending culprit but rather one of the hosts connected to it. While the Honeypot project will detect the Simple Mail Transfer Protocol (SMTP) server as the originator, the SMPT server merely serves as a relay for a large number of connected legitimate business users. This is confirmed when the server's reputation score is checked against a provider such as project Senderbase[73] that was created by CISCO (previously discussed in Section 4.5.5). The results obtained are shown in Figure 4-17. It should become clear that while spam has originated from this server, it retains a good email reputation score and the incidents were it in all probability not due to vulnerabilities on the email server.

IP addresses used to send emails in ○ mweb.net ● 196.28.101.191 /24 Export...

1 - 22 out of 22

IP Address	Hostname	Fwd/Rev DNS Match	Volume		Blacklists	Email Rep.
			Daily	Monthly ↓		
196.28.101.136	a3s1.msp.mm.mweb.net	Yes	4.5	4.7	No	Good
196.28.101.137	a3s2.msp.mm.mweb.net	Yes	4.5	4.7	No	Good
196.28.101.192	osmtp-02.mm.mweb.net	Yes	4.5	4.7	No	Good
196.28.101.191	osmtp-01.mm.mweb.net	Yes	0.0	4.6	No	Good
196.28.101.117	a1s2.msp.mm.mweb.net	Yes	3.4	4.6	No	Good
196.28.101.92	ismtp-02.mm.mweb.net	Yes	3.2	4.5	No	Neutral
196.28.101.91	ismtp-01.mm.mweb.net	Yes	3.0	4.5	No	Neutral
196.28.101.93	ismtp-03.mm.mweb.net	Yes	3.3	4.5	No	Neutral
196.28.101.116	a1s1.msp.mm.mweb.net	Yes	3.0	4.5	No	Good
196.28.101.127	a2s2.msp.mm.mweb.net	Yes	0.0	4.5	No	Good
196.28.101.126	a2s1.msp.mm.mweb.net	Yes	0.0	4.5	No	Good
196.28.101.49	49.101.28.196.mweb.net	No	4.2	4.4	No	Good
196.28.101.48	48.101.28.196.mweb.net	No	4.2	4.4	No	Good
196.28.101.44	44.101.28.196.mweb.net	No	4.3	4.2	No	Good
196.28.101.40	40.101.28.196.mweb.net	No	4.3	4.2	No	Good
196.28.101.42	42.101.28.196.mweb.net	No	4.3	4.2	No	Good
196.28.101.45	45.101.28.196.mweb.net	No	4.3	4.2	No	Good
196.28.101.193	osmtp-03.mm.mweb.net	Yes	4.4	4.2	No	Good
196.28.101.41	41.101.28.196.mweb.net	No	4.3	4.2	No	Good
196.28.101.43	43.101.28.196.mweb.net	No	4.3	4.2	No	Good
196.28.101.194	osmtp-04.mm.mweb.net	Yes	0.0	4.1	No	Good
196.28.101.20	inbound.mm.mweb.net	Yes	0.0	2.0	No	Neutral

Figure 4-17: Senderbase[73] reputation score of 196.28.101.191 on 2014-06-21

[72] http://www.mweb.co.za
[73] http://www.senderbase.org

Initiatives like the Project Honeypot provide a solid base to gain an overview of the activity in a country. There is however the requirement to properly analyze each individual case on a merit bases. A variety of the investigative process tasks can be automated but in many instances it still requires human intervention to assess the situation. This is due to the temporal nature of Internet IP addresses and the large variety of data sources that extrapolate data from incidents.

To illustrate that reliable data sources can often provide conflicting information consider IP address 41.242.112.10. According to the Project Honeypot, the IP address is sending a considerable volume of spam to a variety of international hosts and the host is based in the South African domain. When presenting the very same IP address to the Senderbase project, the results confirm that the IP address is indeed sending volumes of Spam to international recipients but differs in the location of the host. According to the Senderbase project the originating IP is located in Ghana and thus well out of the South African domain with the ISP being Dolphin Telecoms.

4.5.9 OpenResolver for Domain Name Servers

While the Internet is designed so that each device connected is identifiable by a unique Internet Protocol address, humans prefer to use natural language. To address this a service called DNS was created that maps a unique IP address to a unique natural language domain name. Registrars control what IP address a registered domain name maps to. While this is convenient for humans and opens a variety of business opportunities online, the service adds a layer on top of the original addressing scheme thereby increasing the complexity of services to secure. The ability to exploit this added layer of convenience is illustrated in a timeline of attacks presented by (Gilad, Herzberg & Shulman, 2013) in Figure 4-18.

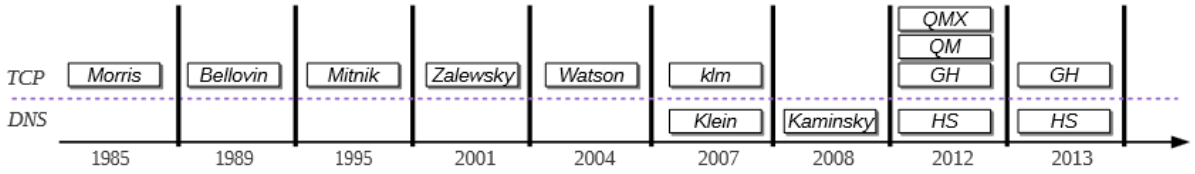

Figure 4-18: Timeline of DNS attacks (Gilad et al., 2013)

The attacks have grown in sophistication but often still operate on attacks with their roots in the previous decade. For example, Smurf attacks were used when the Internet Control Message Protocol (ICMP) was used to query a range of hosts if they knew where a specific host was located (Hudaib, 2014). The hosts queried then attempts to forward

the message received to the intended target, thus creating a amplification of the original request and flooding the target as shown in Figure 4-19.

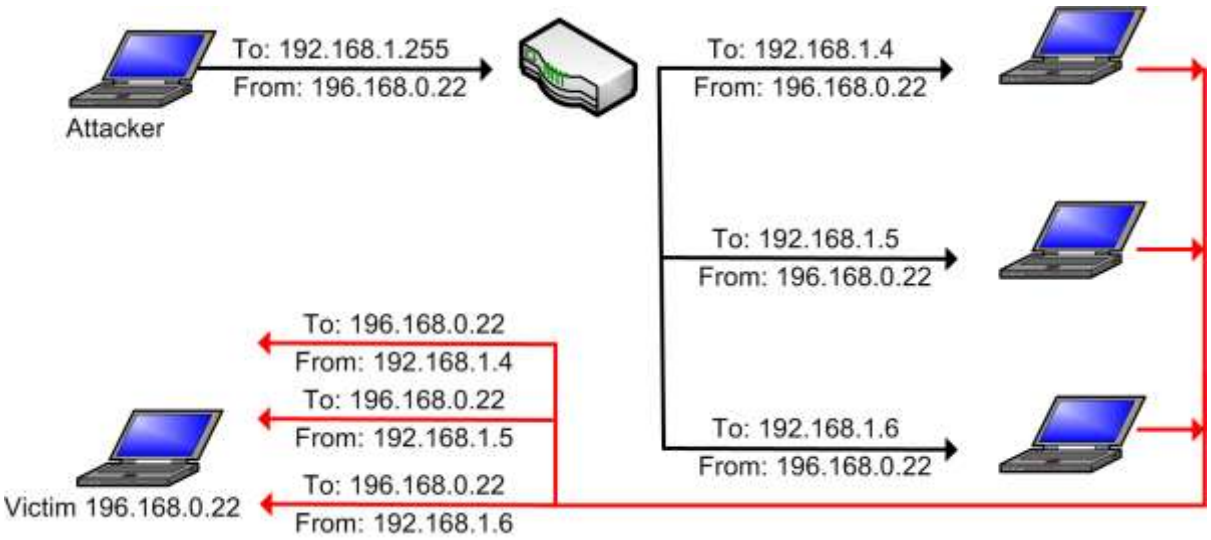

Figure 4-19: Original ICMP Smurf attack

The attack was named a Smurf attack due to the name of the file used to distribute the POC smurf.c[74]. The original ICMP vulnerability has long since been patched and while there are still servers vulnerable to this type of attack it has largely been resolved. Variants of the attack however are still a big threat to the Internet infrastructure and open DNS configurations can assist with DNS amplification attacks in excess of 30GB (Santorelli, 2010). This type of attack only requires that the DNS responds to queries for external hosts, to participate in the attack that is estimated to have an amplification factor of fifty. While there is little threat to the DNS host participating in the attack, the attack itself can potentially bring down specific parts of the Internet.

Determining the amount of DNS servers in a country that are potentially vulnerable to partake in a DNS amplification attack can be estimated by combining the results of two service providers. The Open Resolver Project[75] conducted a scan of the Internet and detected 32 million DNS servers that responded of which 28 million pose a significant threat as of 2013-10-27. The full detected list of the Open Resolver Project is not publicly available, it will only be made available upon request at the discretion of the researchers operating the project. While every effort has been made to contact the project for full access to this list, it has not been successful to date. The web portal does however allow for manual searching in specified subnets.

[74] http://www.rs-labs.com/papers/tacticas/ircutils/smurf.html
[75] http://openresolverproject.org

Comparing the results obtained by the Open Resolver Project with a previous project conducted by Ren, Kristoff and Gooch (2006) yields interesting results. Figure 4-20 was created and illustrates clearly how the number of open resolvers has increased in Africa from the top measured in 2007 to the current situation that was last measured in October 2013 in the bottom.

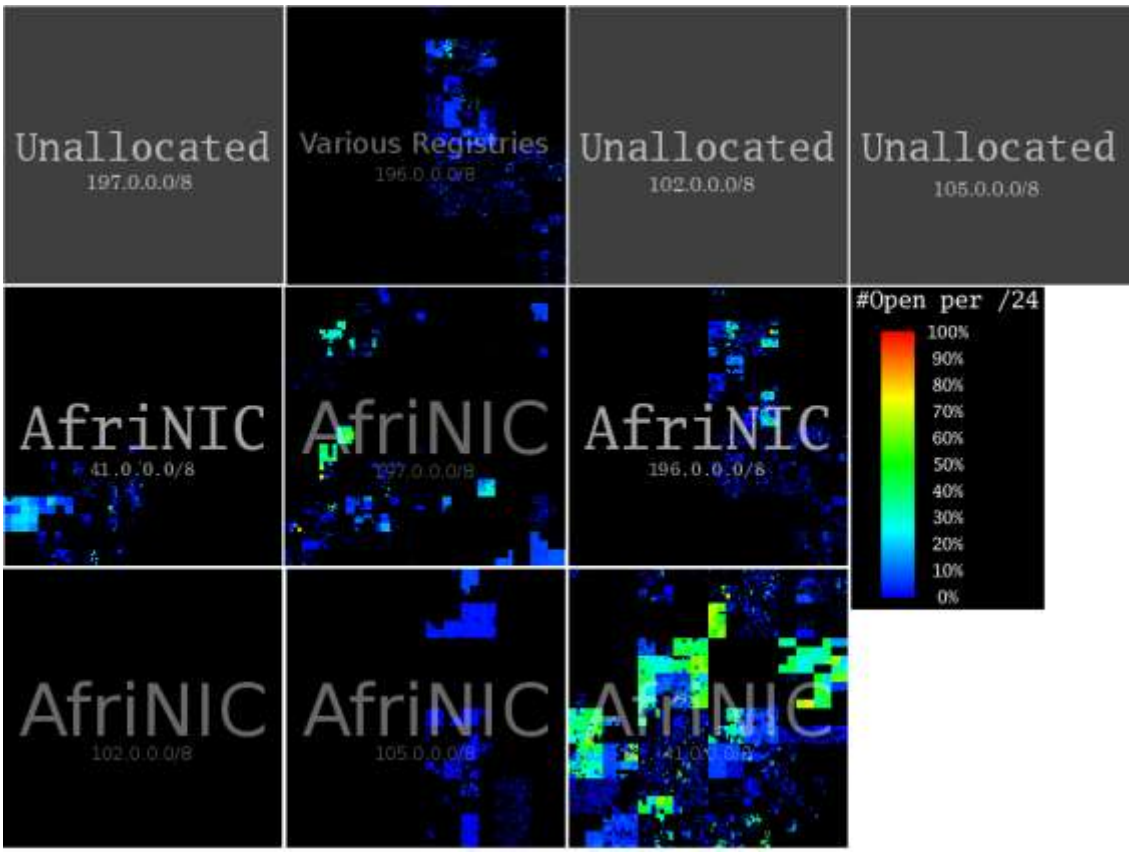

Figure 4-20: Africa's open DNS resolvers 2007-2013 Hilbert Heat map

Detecting open resolvers without scanning or access to the data provided by the Open Resolver project is problematic. The most comprehensive alternative source of data found was the Réseaux IP Européens[76] (RIPE) Atlas project. The project aims to establish the largest ever Internet measurement network to measure Internet connectivity and reachability.

Due to the information available from RIPE Atlas project it is possible to obtain a list of available root DNS and their geographic location as presented in Figure 4-21. The RIPE Atlas project does not classify servers according to any vulnerability, it merely indicates where the DNS servers are located. The results thus still needs to be validated against

[76] https://www.ripe.net

the Open Resolver project to determine if the DNS under investigation is indeed vulnerable to being used in a DOS attack.

Figure 4-21: RIPE project detected DNS servers in South Africa 2014-06-23 [76]

Once a host is selected and submitted for analysis to the Open Resolver Project, the project will return a list of all DNS services that function as open resolvers. The return code (RCODE) is based on the values specified in RFC 2929[77] and has the following possible values:

0. No error condition.
1. Format error – The name server was unable to interpret the query.
2. Server failure – The name server was unable to process this query due to a problem with the name server.
3. Name Error – Meaningful only for responses from an authoritative name server, this code signifies that the domain name referenced in the query does not exist.
4. Not Implemented – The name server does not support the requested kind of query.
5. Refused – The name server refuses to perform the specified operation for policy reasons. For example, a name server may not wish to provide the information to the particular requester, or a name server may not wish to perform a particular operation (e.g., zone transfer) for particular data.

[77] https://tools.ietf.org/html/rfc2929

Any results that returns an RCODE of 0 is considered an open resolver that will respond to queries from outside and can be used in a DNS amplification attack. The results in Table 4-14 lists the associated DNS resolvers queried that were obtained from the initial investigation depicted in Figure 4-21. To obtain the data, the name obtained was translated to an IP address that resolved to 41.79.82.27. By submitting this IP range to the Open resolver project in a /22 subnet range, other potential open resolvers from the same IP range can be obtained.

Table 4-14: IP addresses results from the Open Resolver Project[75] on 2014-06-12

IP Queried	time_t	RCODE	Recursion Available	Correct Answer Provided	IP Responded
41.79.82.26	1403398651	0	1	1	41.79.82.26
41.79.81.42	1403400742	0	1	1	41.79.81.42
41.79.83.114	1403410162	0	1	1	41.79.83.114
41.79.83.115	1403410295	0	1	1	41.79.83.115
41.79.83.116	1403410428	0	1	1	41.79.83.116
41.79.82.130	1403412287	0	1	1	41.79.82.130
41.79.82.174	1403418056	0	1	1	41.79.82.174
41.79.82.186	1403419622	0	1	1	41.79.82.186

While open DNS resolvers are clearly a threat to any infrastructure due to their potential misuse, there is also a very useful application for this type of system for defenders. Consider that botnets make use of URLs to communicate between bots and the host. While a IP address will work, it is static and typically hard to communicate the new address to the distributed bots. A DNS record is preferred since it provides attackers with the ability to change the IP address for the communication infrastructure regularly, thereby effectively hiding the C&C infrastructure. Using DNS is an effective method of detecting their communication since the basic use of DNS always resolves to an IP location (Kara, Binsalleeh, Mannan, Youssef & Debbabi, 2012). To thus detect the spread of a specific malware infection, it could be useful to select a subset of open resolvers in a specific geographic location and query them if they have seen the C&C URL. DNS servers maintain a Time To Live cache for each entry that has been requested of them. If the time to live is not at its maximum, it means the server has not

performed a lookup and therefore has already answered a query for this specific URL recently. By tracking who has answered this prior to the issued request it becomes possible for authorities to track the spread of a specific strain of malware. This approach has been documented for organizational level but can be used on a national level as well by responsible parties (Plohmann et al., 2011).

Significantly more vulnerabilities are available in DNS but most of them are limited to affecting mainly a specific organization or entities reliant on a specific DNS resolver. The potential for national level impact is however present not only in open resolvers but also where zone transfers are available from a DNS server. The number of DNS instances allowing unsecured zone transfers is still high at 11.3% as documented in a DNS survey conducted (Sisson, 2010).

4.6 SUMMARY

While a variety of data sources are available from third parties, significant limitations exist in almost all of the data sources examined. The data sources provide valuable information but care should be taken with the interpretation of any given dataset. Specialized data sets such as those found in the OpenResolver project provide comprehensive data sets per region due to the nature of the data. Data obtained from Phishtank however should not be taken at face value and will require significant processing to achieve accurate statistics from. The fundamental difference between the two data sources is the manner in which it is possible to measure the potential problem. An open resolver will definitely answer when queried for a DNS address or else it is not classified as an open resolver. Phishtank has a whole range of other considerations such as location, language and message content to consider before a classification can be made.

False positives can be found in almost all of the datasets in some form. Even specialized data sources such as Shodan are not excepted from providing false positives since there are software allowing system administrators to change the device fingerprint returned. The will cause Shodan to provide a false positive when individuals query the database. The data is not without use, however, and is still the best available source of data regarding the state of a countries Internet facing infrastructure.

Part I of this research document discussed the need for national cybersecurity initiatives, current national cyber strategies proposed and their current implementation limitations in Chapter 2. The possible attack surfaces of a nation and the role that open

source information datasets could provide was explored in Chapter 3. Following this, a detailed examination of potential data sources relating to the attack surface on a nation was performed in Chapter 4 to establish applicability and limitations of identified data sources.

Building on the information obtained in Part I, Part II of this document will further explore the potential use of the datasets evaluated in Chapter 4 to address the needs and limitations identified in Chapters 2 and 3. Next, Chapter 5 introduces a fusion model that can provide a best guess representation of devices, data and vulnerabilities available at a given point in time for a given country. A subset of the data sources examined in Part I of this document will be applied to the proposed fusion model. Validation of the model is performed by means of case studies presented in Chapters 6 and 7.

PART II

Experiment design and implementation

The user is going to pick dancing pigs over security every time.

Bruce Schneider – Cryptographer, security and privacy expert

5

Data fusion, model and architectural design

5.1 INTRODUCTION

A number of seemingly disparate data sources were examined in Chapter 4. Each data source examined provided information relating to a specific vulnerability in the attack surface categories on a national level. Unfortunately, no single data source provides all the required information, therefore establishing the need to combine information. To obtain a clear view of the combined intelligence that the data sources could provide, requires a disciplined approach often lacking in the cyber domain.

The research field of data fusion on the other hand provides established models and frameworks that aid multi source information intelligence system design. A brief introduction to data fusion is provided in Section 5.2 that provides the terminology, limitations and background information applicable for data fusion.

Achieving data fusion on a national level requires a systematic approach to data source selection and to cyber sensor data fusion methodology. As such, this chapter discusses the design of the implemented experimental system which was based on an adapted version of the Joint Directors of Laboratories (JDL) model (discussed in Section 5.5). This chapter contains relevant information such as Entity Relationship Diagrams (ERD), code snippets, database queries and other relevant information as required.

5.2 DATA FUSION INTRODUCTION

Data fusion is defined by White (1991) as "*A multi-level process dealing with the association, correlation, combination of data and information from single and multiple sources to achieve refined position, identify estimates and complete and timely assessments of situations, threats and their significance*". The terminology 'data fusion' and 'information fusion' are often used interchangeably but can have variations depending on the situation (Castanedo, 2013). In instances where the terminology are

distinct, the distinctive characteristic is the level of information processed. Data fusion typically makes use of information at a raw level directly from a sensor whereas information fusion makes use of already processed data. This distinction becomes evident when considering a definition for information fusion: "*The study of efficient methods for automatically or semi-automatically transforming information from different sources and different points in time into a representation that provides effective support for human or automated decision making*" (Khaleghi, Khamis, Karray & Razavi, 2013). This research will make use of the term data fusion to describe the fusion process since the data obtained from the various cyber sensors described in Chapter 4 is used as directly as possible.

Data fusion and information fusion should also not be confused with data mining since the focus areas of the two fields are different. Waltz (2003) describes data mining as a knowledge discovery process that differs from data fusion on inference method and temporal perspective, but notes that both are required in a practical intelligence application. Data fusion makes use of known patterns while data mining attempts to infer these previously unknown patterns from datasets. The successful application of data fusion techniques has been presented in a variety of fields ranging from transportation optimization (Anand, Ramadurai & Vanajakshi, 2013) to military situational awareness (Blasch, 2013). The application of data fusion in the cyber domain is further discussed in Section 5.3.

5.3 DATA FUSION MODEL SELECTION

Data fusion in the cyber domain has been conducted previously with Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) and achieved good results. More recent work aimed to incorporate soft fusion techniques that integrate the human component in the data fusion process (Hall, McNeese, Hellar, Panulla & Shumaker, 2009). One of the most challenging aspects of data fusion occurs when the reliability of data sensors are not equal. The reliability aspect of information fusion has been discussed at length with a variety of proposed solutions offered such as Dempster Shafers method and derivatives such as the Transferrable Belief model (Smets, 1993). Work in the cyber domain that makes use of reliability fusion algorithms has to date only been conducted on host level systems and not on organizational or national level.

Various models exist that are applicable to the proposed experimental system. Models that provide structure on how data sources should be evaluated, how data fusion should occur

and how situational awareness can be optimized are all relevant. There are however limited research that explain and transform these existing models in a manner that they are applicable to the cyber domain (Giacobe, 2013). While at first glance it might seem an unreasonable requirement to re-evaluate each model for its application to the cyber domain, the need exists. There is a distinct need to re-evaluate each model for its applicability to the cyber domain purely because of the distinct differences of the physical world vs. the cyber world. While in the physical world sensors are based on the laws of physics and information is available on how to measure characteristics such as resolution, detection performance and reliability, the cyber domain is not as evolved yet.

A few of the well known models such as the JDL and Waltz models have been discussed for their applicability in the cyber domain (Bass, 2000; Schreiber-Ehle & Koch, 2012). In nearly every examination encountered, the original model was to some degree applicable to the cyber domain but required some changes in either terminology or application. These changes do not alter the flow of the model significantly, but are required to suit the cyber domain. Even with the examination of the various models' applicability to the cyber domain, a variety of problems exist in making use of these models in a practical manner. Very little previous work exists beyond data fusion of IDS and IPS systems as first observed by (Giacobe, 2013). As a result of this, selection of the best fit models for data fusion on a national level is at best an estimation of probable fit. The selection of the JDL model was guided by similar research examining the state of critical infrastructure on a national level (Timonen, Lääperi, Rummukainen, Puuska & Vankka, 2014). An example of the complexity of evaluating cyber sensors according the traditional measurements will be presented in Section 5.7.1. The examination section will make use of the adapted Waltz model to evaluate a potential cyber sensor. This will be done in order to highlight the complexity in making a quantifiable assessment according to traditional Electronic Warfare (EW) model criteria. Criteria that are easily quantifiable in the EW / physical domain, are much more abstract in the cyber domain and quantification is probability based.

There is no denying, however, that in order to achieve effective data fusion, a formalized model will be required. The variety of data sources are sufficiently diverse that any system created, will not be able to function in the long term without some form of guidance. Taking into account the above requirements and discussed constraints, the JDL model was selected for implementation in this research. The choice of the JDL model can be attributed to the existence of prior research validating its potential and will be discussed in Section 5.4. The application of the JDL model has been discussed in the cyber domain in contrast with other

available models (Schreiber-Ehle & Koch, 2012). There are also a number of published research applications in the cyber defense domain based on the JDL model to draw from. Other work that influenced the system design included the Waltz model for sensor classification and Endsley's situational awareness theory (Endsley, 1995).

5.4 THE JDL MODEL MAPPING AND IMPLEMENTATION

The JDL model was created to facilitate the fusion of multi-source sensor data in a structured manner (Steinberg, Bowman & White, 1999). Various other models exist that could potentially be used as the basis for such a fusion system and they are briefly discussed below. The adapted Waltz model (Bass, 2000) and the Transferable belief model (Smets & Kennes, 1994) are also possibly applicable to the cyber domain. The 1992 version of the JDL model is depicted in Figure 5-1.

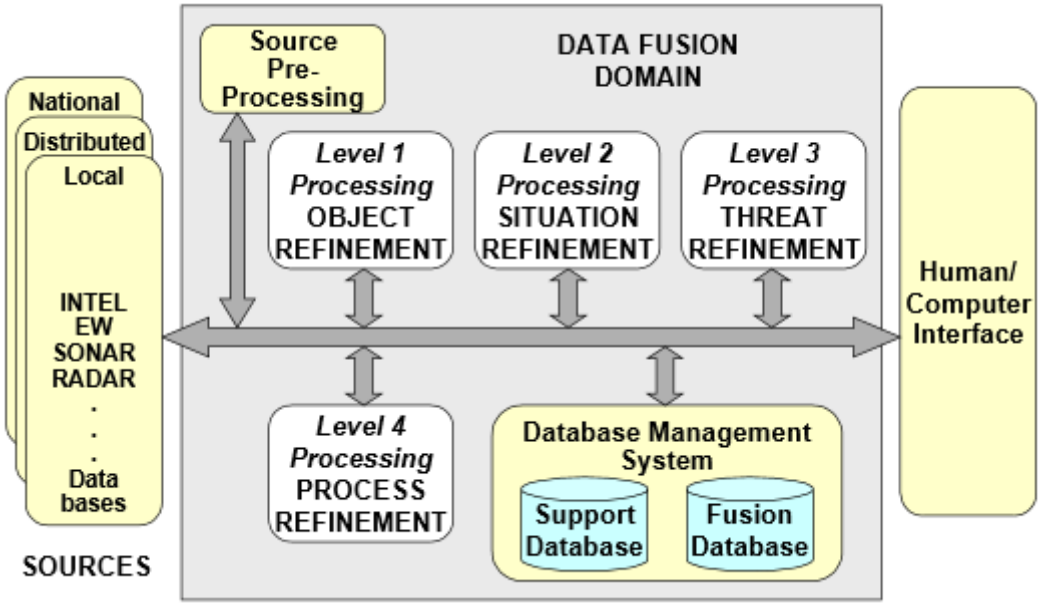

Figure 5-1: Original JDL model, 1992 version (Hall & Llinas, 1997)

The original JDL model was specifically designed for EW functions such as multi sensor data fusion that is commonly performed. The first observed use of the JDL model in cyber security was in an experiment where the alerts of multiple IDS systems were combined to achieve fewer false positive alerts in a networked environment (Schreiber-Ehle & Koch, 2012). This work resulted in the adapted version of the JDL model as seen in Figure 5-2. While retaining all the levels of data processing from the original version of the JDL model, this model was tailored more towards networked cyber environments.

At level 0 of the adapted JDL model, all relevant information was processed to result in information regarding the objects under observation in the cyber domain. The described objects were further processed at level 1 of the JDL model to depict the objects in greater detail. At level 2 the focus shifted from just observing objects to incorporating information regarding the current situation. To achieve this, metadata sources containing information regarding vulnerabilities, known malware signatures and other data sources were incorporated. level 3 is described as the level responsible for future threat assessment (Schreiber-Ehle & Koch, 2012). level 4 provides the opportunity for sensor management and at level 5 visualization and process refinements is depicted. This interpretation of the JDL model introduces metadata sources and moves the process improvement step to level 5. Traditionally the improvement process is located at level 4 as opposed to level 5 in the adaptation.

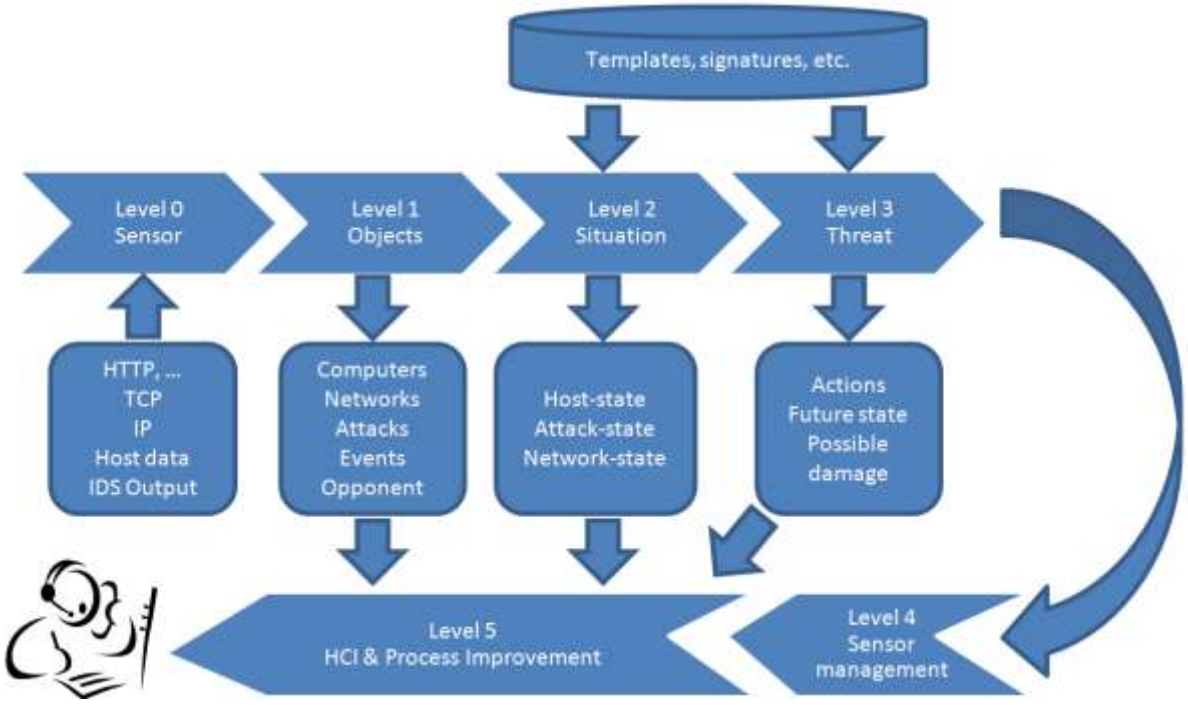

Figure 5-2: Cyber adapted JDL model (Schreiber-Ehle & Koch, 2012)

5.5 ADAPTATION OF THE JDL MODEL FOR NATIONAL CYBER FUSION

Derived from the work presented by Schreiber-Ehle and Koch (2012), the model depicted in Figure 5-3 describes the current experimental system. The model largely remains the same but takes the work of Giacobe (2012) on first order entity extraction into consideration. This results in two variations introduced on the previous model illustrated in Figure 5-2.

The most significant adaptation is that the objects identified at level 0 and level 1 are objects as opposed to properties of the identified objects. The rationale behind this change is not complex and similar in concept to object orientated programming theory. Consider that an attack event in the cyber domain is based on the communication flow occurring between two hosts. Thus, the attack itself is not an object but rather a property of at least two objects. Similarly, vulnerability detected on a host is not a object, but rather a property of the object it is associated with. To cater for this distinction, the objects identified at level 1 in Figure 5-3 can relate to objects such as computers, devices, adversaries or even information regarding humans.

The second adaptation is the earlier inclusion of metadata sources such as vulnerability data. This allows for greater population of properties on lower levels of the JDL model in order to obtain better results at higher levels. Prior work conducted by Giacobe (2012) focused on first order entity extraction and as an example, vulnerabilities were matched to selected entities at level 1. This provides level 2 with the opportunity to focus on the situation since the properties of the entities in level 1 has been populated as far as possible.

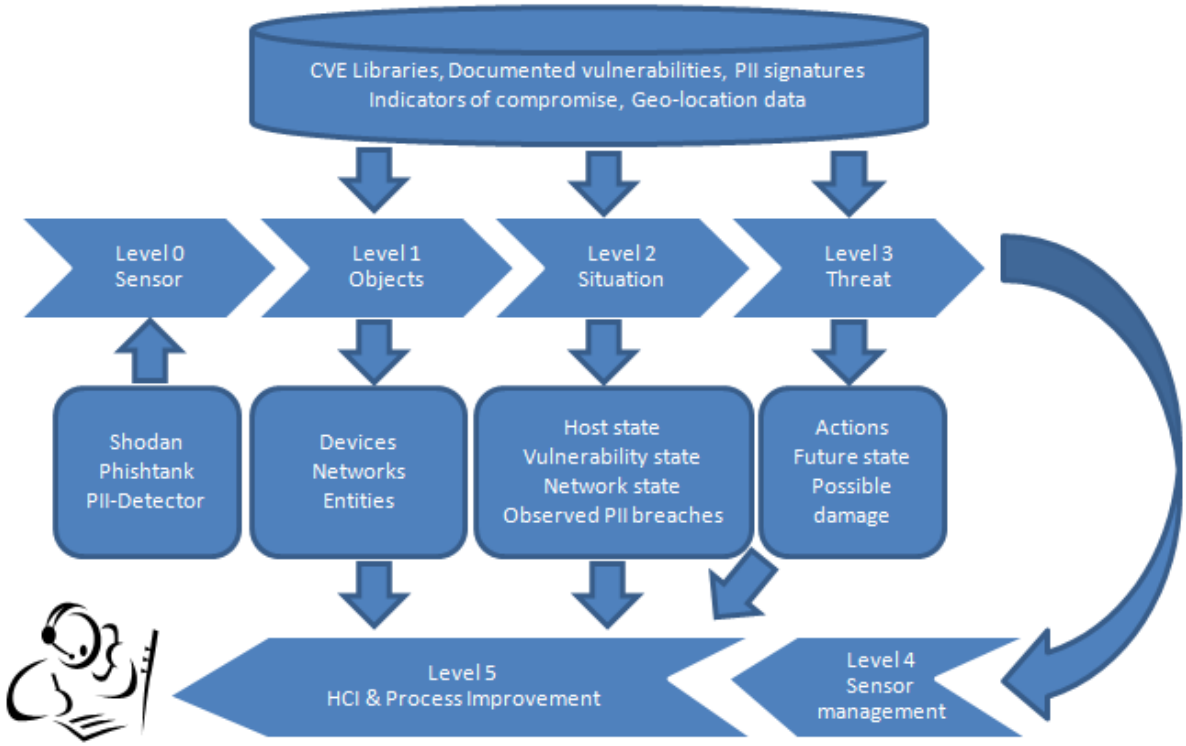

Figure 5-3: Adapted JDL model to facilitate the fusion of national level data sources

The following sections will examine the role of each of the JDL model levels as it pertains to the cyber domain. In conjunction, data source evaluation and the architecture of the experimental system is presented.

5.6 SENSOR SELECTION

A variety of potential data sources that can be used on a national level in the experimental system was discussed in Chapter 4. Each data source's potential information output was described, but due to practical limitations, not all data sources could be utilized in this experiment. Factors such as data accessibility, cost, integration effort all had to be considered in the evaluation when considering the suitability of a information source. For example, some datasets such as those from Shodan discussed in Section 4.4.2 are available, but exporting large volumes at a regular interval can become prohibitively expensive. Data sources such as Builtwith previously discussed in Section 4.4.1 do not allow custom searches, placing a limitation on the volume of data available. Data sources such as those available from the geolocation services examined in Section 4.5.2, are both available and easy to integrate but requires at least monthly updates to remain informative and accurate. The factors mentioned, all contribute to the operational cost of monitoring for vulnerabilities on a national level.

In addition to the limitations discussed above, each selected data source had to provide information relating to the components that make up the attack surface of a nation as discussed in Section 3.2. The Shodan data source discussed in Section 4.4.2 provides ample information regarding available hardware devices, their associated firmware and also software deployed on these devices. Data sources such as PhishTank and DataLossDB discussed in Section 4.4.5 and 4.4.8 could provide information relating to the people component of the attack surface, but examination revealed poor data quality from both sources for the South African domain. This presented a significant problem for the purpose of this research and required the implementation of a custom sensor. The developed sensor had to comply with current legislation in a similar manner as all other sensors evaluated. Thus, no scanning could be performed. Only open source data could be utilized to supplement the information related to the people category of the attack surface. The sensor developed is referred to as the 'PII detector' and will be discussed in greater detail in Section 5.14.2 with results of the sensor's performance in Chapter 7.

Given the requirements for sensor selection and the limitations of the examined data sources, the following data sources were selected for implementation in the experiment to act as sensors in the fusion process.

Primary cyber data sensors:

- Shodan
- Maxmind geolocation library
- Custom PII detector

Metadata available for the selected cyber data sensors:

- NIST CVE library
- Custom Leet speak dictionary
- PII signatures library

The data sources selected each provide information relating to the attack surface of a nation. The information provided by each sensor is mapped to the corresponding attack surface in Figure 5-4. Since the metadata sources are typically only used to enrich the properties of the objects defined in the JDL model, they are not all included in the diagram.

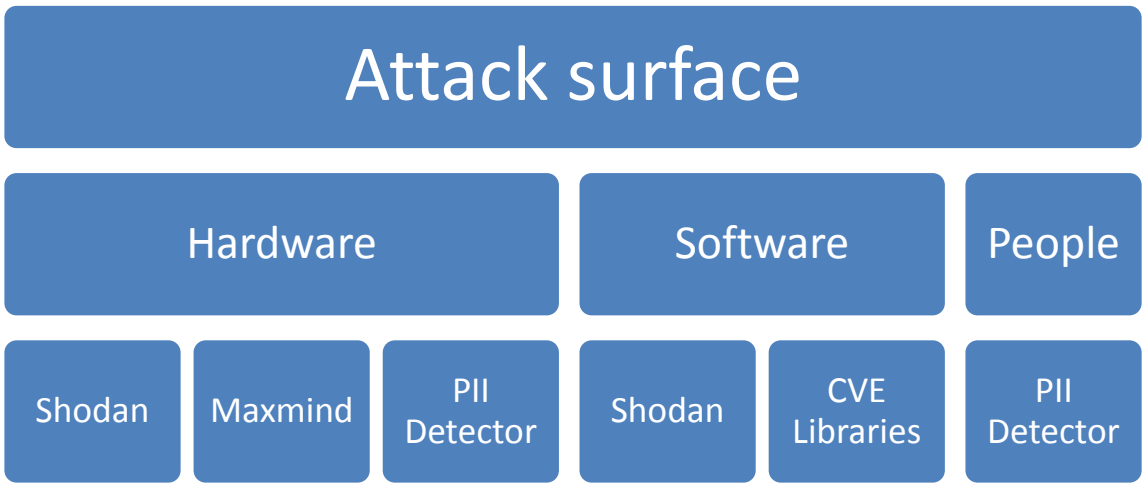

Figure 5-4: Sensor information to attack surface mapping

This section focused on the selection of data sources for the fusion process and examined how the selected sources map back to the attack surface of a nation. Section 5.7 will examine the potential evaluation of the selected sensors as performed in traditional data fusion environments.

5.7 SENSOR EVALUATION

Normal applications of the JDL model have the ability to select sensors based on their complementing characteristics. A model that exists to facilitate the measurement of traditional sensors for suitability is the generic Waltz model (Waltz & Llinas, 1990). The Waltz model originally examines data sources based on the following conditions:

- Detection Performance
- Spatial/Temporal Resolution
- Spatial Coverage
- Detection/Tracking Modes
- Target Revisit Rate
- Measurement Accuracy
- Measurement Dimensionality
- Hard vs. Soft Data Reporting
- Detection/Tracking Reporting

Extending the work to make it more suitable for the cyber environment, required the re-interpretation of a few elements from the original Waltz model. This work was performed by Bass (2000) and resulted in the following adaptation.

- **Detection Performance** – The detection characteristics, i.e. false alarm rate, detection probabilities and ranges, for an intrusion characteristic against a given network centric noise background. For example, when detecting malicious activity, non-malicious activity may be modeled as noise.
- **Spatial/Temporal Resolution** – The ability to distinguish between two or more network-centric objects in space or time.
- **Spatial Coverage** – The span of coverage, or field of view of the sensor. For example the spatial coverage of a system log file is the computer system processes and system calls being monitored.
- **Detection/Tracking Modes** – The mode of operation of the sensor, i.e. scanning, single or multiple cyber object tracking; or multimode operation.
- **Target Revisit Rate** – The rate at which an "i-object" or event is revisited by the sensor to perform measurements.
- **Measurement Accuracy** – The statistical probability that the cyberspace sensor measurement or observation is accurate and reliable.

- **Measurement Dimensionality** – The number or measurement variables for network object categories.
- **Hard vs. Soft Data Reporting** – The decision status of the sensor reports, i.e. can a command decision be made without correlation or does the sensor require confirmation?
- **Detection/Tracking Reporting** – The characteristic of the sensor with regard to reporting cyber events. Does the sensor maintain a time-sequence of the events?

Obtaining the required information regarding all examined data sources is possible with extensive experimentation and validation. The process will be both a costly and a time consuming undertaking. With this in mind, the research presented here acknowledges the need for formal assessment of data sources but selected to focus on what can currently be achieved. As discussed in Chapter 4, every effort was made to incorporate previous assessments from literature to at least partially validate the findings of this study. Formal assessment of the data sources might reveal additional characteristics of selected data sources but should not negate the potential for the fusion process proposed. As an example to illustrate the potential cost and time allocation formal validation of each data source will require, the Shodan sensor will be examined.

5.7.1 SHODAN WALTZ MODEL ASSESSMENT

In this section the Shodan cyber sensor will be examined against the criteria presented in the Waltz model to illustrate the complexity of measuring a sensor in the cyber environment.

- **Detection Performance** – A variety of devices are located on the Internet but to obtain an indication of the performance of this sensor, an indication of the total number of devices in the South African domain would be required. Since there is no specific numbers available regarding this type of distribution, it would be at best an estimate of the performance of this sensor's detection. If any competing service existed that provided similar information, statistical inferences could be used to estimate the number of devices. No such competing service could be located and therefore this is not a possibility. It should be noted that while it is not possible to estimate the current number of devices, Shodan is still the most comprehensive public source of information.
- **Spatial/Temporal Resolution** – While Shodan appears to present the ability to monitor multiple net-centric devices in both space and time, verification of this

ability is problematic. Given that devices appearing in the Shodan dataset is Internet facing devices and available on a national level, time and distance constrains are introduced. While it is possible to verify devices geographically close to the author, obtaining a measurement for the accuracy on a national level requires multiple contact sessions with a variety of entities. Difficulty in gaining access to information only available from these entities are presented not only by their geo-distributed nature but also by their organizational structure. Many individuals and organizations react adversely when contacted by security researchers and thus to find willing participants will require an extended period of time not afforded by this study.

- **Spatial Coverage** – The coverage of the Shodan dataset is class-leading at present and growing in the author's opinion. The field of view spans a multitude of geographic boundaries and IP ranges and is not limited by device type. However, coverage in the cyber domain is hard to quantify. Aspects such as darknets, the inability to effectively scan IPv6 extended ranges and defensive technology such as firewalls limit the ability to provide a credible assessment of coverage.
- **Detection/Tracking Modes** – The Shodan sensor is classified as a scanning sensor due to the operational procedure. There is not a continuous data feed aimed specifically at a specific target but information regarding objects are relayed when the application examines the IP space the device occupies.
- **Target Revisit Rate** – The Shodan website states that records are refreshed at least every three months. However there are several instances in the current datasets where devices have been refreshed once a month and other instances where there is no continuous occurrence of a previously detected device.
- **Measurement Accuracy** – The only method of obtaining measurement accuracy for the Shodan sensor is to obtain a snapshot of the current dataset and examine the results for accuracy via manual inspection. Due to the large volume of data available and the constraints regarding spatial coverage, measurement of this point is also problematic. While it is possible to examine devices geographically close to the author, this represents an almost insignificant volume compared to the complete dataset.
- **Measurement Dimensionality** – A variety of measurements are performed by Shodan and the dataset contains information regarding hardware and software

present on a specific IP address. Information regarding the operating system, device model and manufacturer, services present and geolocation is available

- **Hard vs. Soft Data Reporting** – A variety of factors influence the measurement of this category. The sensor reports that a device is present on a given IP address at a certain time. This drives the potential that this sensor can be used to make decisions without further investigation. The problem however is that there are a variety of factors that influences the data accuracy and as such it is classified as a soft sensor in the opinion of the author. The scanning nature of the Shodan system means that it is not a real time sensor and that the detected device could have received a new IP address or it could have been disconnected. Further considerations such as emerging active defense decoys complicate the classifications presented by Shodan.
- **Detection/Tracking Reporting** – The Shodan system provides comprehensive time-sequence of events relating to a device from first detection to last.

In summary, assessing cyber sensors at a national level is time-consuming and difficult to perform with limited human resources. This does not, however, negate the potential benefit that could be obtained from the fusion of these data sources. The JDL model is a continuous improvement process that requires data sources and the data fusion process to be continually adjusted for better accuracy. While the data presented for use at level 0 of the JDL model in this experiment is hard to classify and limited to only a specific geographic region, the fusion process still presents more situational awareness that any single data source currently provides. Evaluation of the data fusion process and data sources can be extended significantly. Khaleghi et al. (2013) presented common problems associated with the data fusion process and Rogava et al. (2010) presented an ontology for data source evaluation as illustrated in Figure 5-5.

Section 5.8 and higher will move the focus from the data sources to examine the JDL model on a per level case. The examination will provide information regarding the original purpose of the JDL model as well as how the model is applicable to the cyber domain.

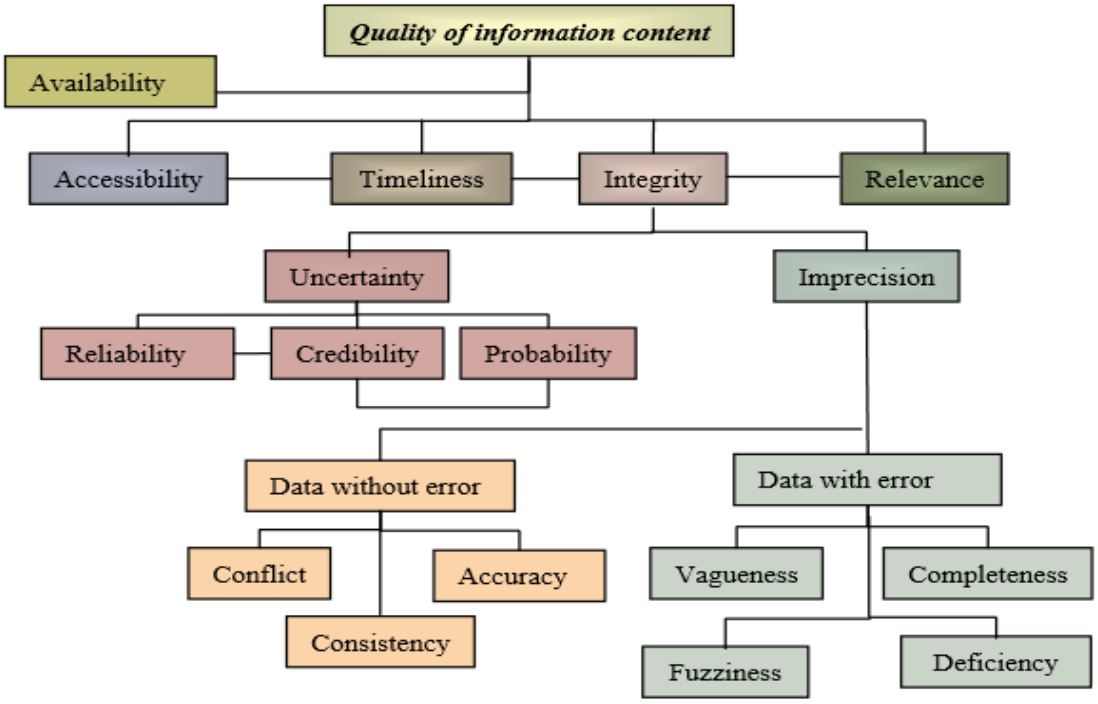

Figure 5-5: Information quality ontology as described by Rogava et al. (2010)

5.8 JDL LEVEL 0 - SENSOR

Level 0 of the JDL model generally deals with sub object data association and estimation (Steinberg et al., 1999). The main purpose of this level is to combine signal output information regarding the characteristics of the object under observation. Since the cyber domain is a unique man-made construct, traditional sensors only provide a limited view into the cyber domain. For further information gathering new sensors are required. A sensor in the cyber domain can be defined as a sensor that monitors cyberspace (Gagnon, Truelove, Kapadia, Haines & Huang, 2010). This definition is also stated by O'Grady, Murdoch, Kroon, Lillis, Carr, Collier and O'Hare (2013) but they add that the sensor must be a software based sensor.

Cyber sensors have the ability to produce data in a large range of formats and describe a wide variety of information similar to traditional sensors. Data types from cyber sensors available for data fusion can range from communication packet headers, to timestamps of files or the vulnerability level of a given device (Giacobe, 2010). The granularity of the information supplied to the JDL model at level 0 can vary to contain either processed output or raw data (Schreiber-Ehle & Koch, 2012). Regardless of the granularity, the purpose of level 0 is to perform data alignment and the creation of the entities and their associated properties existing in cyberspace.

The following section will discuss the purpose and architecture of the JDL model level 1 as applicable to this research.

5.9 JDL LEVEL 1 - OBJECTS

Level 1 of the JDL model is traditionally concerned with object refinement by combining raw level data to obtain a better understanding of the object under observation (Steinberg et al., 1999). This process is also referred to as first order entity extraction in the cyber environment and properties of these identified entities are typically IP address, host names, etc. (Giacobe, 2012). Although the entities were already created at level 0 of the JDL model, this level serves to enrich the properties of the created entities. A fundamental aspect of representing data at this level is by means of entity relationships that maps an entity to all relevant properties. Although traditional representations such as taxonomies, binary and family trees are effective at this level, database queries can comfortably represent the required relationships (Bass, 2000). The structure of these database queries is relatively generic SQL representation such as:

SELECT (attribute) FROM (table) WHERE (condition)

This selection of an identified entity allows easy manipulation and creates the opportunity for further enrichment. It is at this level that all information made available by the cyber sensors needs to be added as properties to the identified object. Examples of the types of information that could be added can be found in the vulnerability datasets such as CVE lists maintained by NIST. The enrichment of the identified object with vulnerability information was previously described by Giacobe (2012), when Nessus results were used as basis for the fusion experiment. By altering the dataset to use Shodan data and using CVE lists as the vulnerability information, it becomes possible to replicate the host based experiment to a national based experiment. It should be noted that while CVE information is useful to identify potentially vulnerable hosts, other factors need to be considered. For example, just because a host is indicated as vulnerable does not mean the host is vulnerable. Several factors such as the protection mechanisms deployed on the host needs to be taken into account as well (previously discussed in Section 4.5.7). The generic fusion process of matching Shodan data to NIST CVE data is depicted in Figure 5-6. Matching of data can only occur once all data is already imported into the database as described in Section 5.8.

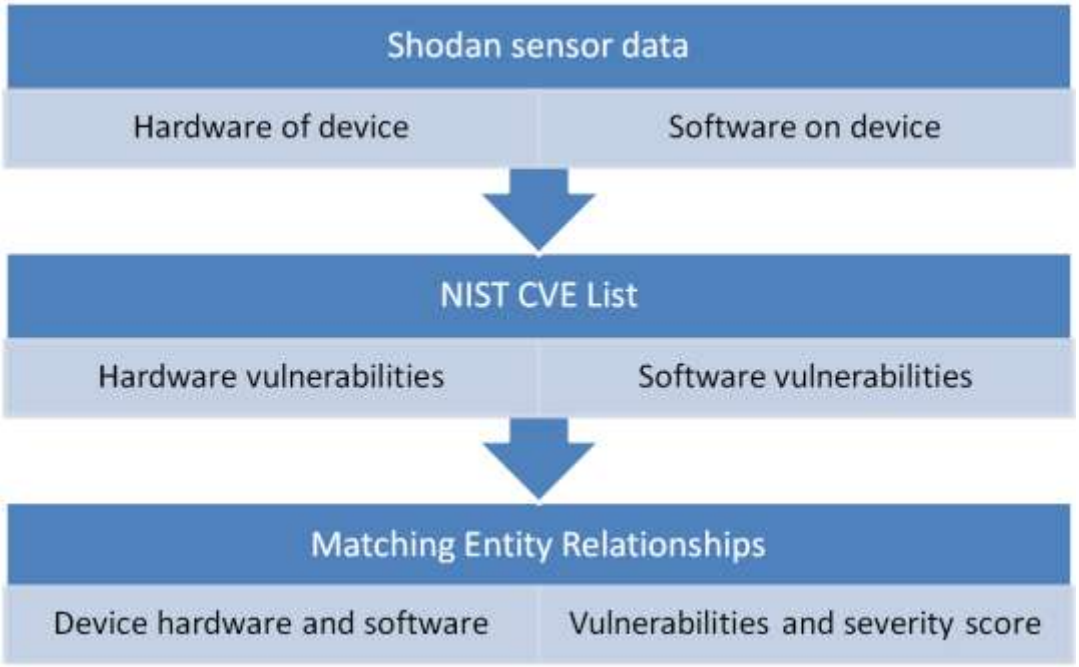

Figure 5-6: Host information and CVE data fusion process flow

While CVE data is a good indicator that a vulnerability might exist, it cannot indicate that a host has already been compromised. For this type of information data sources such as Indicators Of Compromise (IOC) descriptions can be beneficial. The information contained in these IOC descriptions could be used to examine hosts identified at level 0 for potential existing breaches. Examples of IOC descriptions can be found in reports of malware operation, such as the Stuxnet report that indicated specific ports were used by the malware (Falliere et al., 2011). Unfortunately most current indicators of compromise focus on host-based detection requiring the need for access to the host under investigation. There are however instances available that could be used to identify external facing entities that have been compromised. An example of such an IOC is presented in Figure 5-7 showing the R57 web shell commonly used by hackers to retain access to a server.

In summary, level 1 is thus responsible for matching all possible information regarding the identified object in level 0 and mapping it to the required properties of the object. The information can be from a wide range of sources as long as it describes some aspect of the object. The following section will describe the role of level 2 in adapted JDL model as depicted in Figure 5-3.

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <short_description>Backdoor-r57shell</short_description>
  <description>IOC to detect r57shell. can be used as a backdoor or remote administration tool, or for
  <authored_by>Cedric PERNET</authored_by>
  <authored_date>2012-05-16T09:29:23</authored_date>
  <links>
    <link rel="category">Backdoor</link>
  </links>
  <definition>
    <Indicator operator="OR" id="bb1128ac-96ba-4f4a-bea3-fc804000d384">
      <IndicatorItem id="c9e9c835-8bfe-418e-93e6-7742b0118b0a" condition="contains">
        <Context document="FileItem" search="FileItem/StringList/string" type="mir" />
        <Content type="string">r57shell</Content>
      </IndicatorItem>
      <IndicatorItem id="9723143d-46b5-4062-900a-4c92b9d2b735" condition="contains">
        <Context document="FileItem" search="FileItem/StringList/string" type="mir" />
        <Content type="string">$filename = @basename($_POST['loc_file']);</Content>
      </IndicatorItem>
      <Indicator operator="AND" id="9c709b3b-3867-4f2d-8a32-3ee89f2cf2c2">
        <Indicator operator="OR" id="e28db126-4db9-4909-94d9-0f25ea107b4f">
          <IndicatorItem id="b23f2773-848b-4134-b755-412f6921cca8" condition="contains">
            <Context document="Network" search="Network/String" type="network" />
            <Content type="string">r57shell</Content>
          </IndicatorItem>
          <IndicatorItem id="c956b3b9-3398-4f01-a578-fb1d522cd32c" condition="contains">
            <Context document="Network" search="Network/String" type="network" />
            <Content type="string">&amp;cmd=edit_file&amp;dir=</Content>
          </IndicatorItem>
          <IndicatorItem id="e9f9f75a-0e0f-4cb2-a120-0d29c2f0f0a8" condition="contains">
            <Context document="Network" search="Network/String" type="network" />
            <Content type="string">&amp;cmd=php_eval&amp;submit</Content>
          </IndicatorItem>
        </Indicator>
      </Indicator>
    </Indicator>
  </definition>
</ioc>
```

Figure 5-7: Indicator Of Compromise for R57 web shell

5.10 JDL LEVEL 2 - SITUATION

Level 2 of the JDL model focuses on identifying and mapping the relationship between entities and events in the observed situational environment (Steinberg et al., 1999). This level is generally concerned with clustering and relational analysis of the current status by building on the information obtained in level 1 processing. The output of this level does not have to be a complex set of evaluations, it could simply be an indicator on the state of the object or objects under evaluation (Schreiber-Ehle & Koch, 2012).

The information presented at this level should thus not focus on any specific object identified in level 0 and refined in level 1. It should aggregate information regarding the situation of the current environment. Expressing this in a SQL statement for

illustrative purposes will include aggregate and summative functions such as sum or average and potentially, group keywords.

SELECT COUNT(aggregate) FROM (table) WHERE (condition) GROUP BY (aggregate)

Consider the IOC data described for use at level 1 to create a property in a object identified at level 0. Should an IOC match be found on the host, the object will have a property that could be set as compromised. At level 2, the observable environment is important and therefore the total number of compromised hosts versus the number of normal hosts is important. It is at this level where analysis will occur for relationships between hosts with certain properties. Another potential function of level 2 is to examine hosts according to their distribution in a geographic region. While the demarcated cyber domain is the full national operating environment, the ability to cluster objects in geographical location is beneficial as described in sections 2.7 and 4.5.2.

The function of level 2 is thus to group and to perform analysis on the objects populated in level 1. The focus shifts from the individual object, to all objects identified in the fusion system. The following section examines the role of level 3 of the adapted JDL model.

5.11 JDL LEVEL 3 - THREAT

Level 3 of the JDL model, aims to make use of currently available information to infer possible future states of the system under observation (Steinberg et al., 1999). One of the key differences between level 2 and level 3 is that at level 2 of the JDL model time is not regarded as a factor (Tadda & Salerno, 2010). This is in contrast with level 3 that aims to predict future state and potential attacks based on information made available by prior levels. Level 3 builds on the information obtained from levels 1 and 2 to examine the potential future state of the overall system, not just an individual component (Giacobe, 2010).

CVE lists or open alternative open source vulnerability data sets can once again be employed to determine the extent of certain vulnerabilities on individual entities. While the identification of vulnerabilities is strictly speaking a level 1 action, with additional information it could also serve on level 3. Consider real time attack sources as previously discussed in Section 4.5.6. These data sources provide information regarding current attacks on infrastructure. By examining the attack characteristics such as

vulnerability exploited in the attack and fusing that information to currently known vulnerabilities, the potential for future state predication will become possible. Any host that suits the vulnerability profile for the observed attack could be identified and marked as potential future victim. Based on the vulnerability descriptions and the observed attack methodology, it might be possible to infer the potential next targets and send out an alert in advance to potentially affected parties.

Level 3 is thus similar to level 2 but with an added temporal component dependency. It serves to aggregate available information but also has the function to predict the future state. The outcome of this level could be the indication that a successful attack against the network under evaluation has been made, but that the network will continue to work efficiently (Schreiber-Ehle & Koch, 2012). The following section will describe the role of level 4 in the adapted JDL model.

5.12 JDL LEVEL 4 – SENSOR MANAGEMENT

Level 4 of the JDL model is a management layer that influences sensor selection, sensitivity and input parameters (Steinberg et al., 1999). Not all information is applicable all the time, and as such, the requirement might exist to not use one specific cyber sensor. In other instances, the system might have to respond in a certain manner if a specific event is detected. Regardless of the type of response required, level 4 can implement either manual or automatic operational requirements (Timonen et al., 2014). In an effort to relate the purpose of this level back to prior levels, consider the vulnerability matching process performed on level 1. At level 4 the vulnerabilities to be matched will be directly controlled by specifying what time-span of CVEs available should be used. This action will directly influence the number of vulnerabilities reported by the system as the dataset is either increased or decreased.

In summary, level 4 is responsible for function such as event response control, filtering of data and data source selection. It has the potential to manipulate the objects identified in level 0 by including and excluding data sources from the fusion process. In the next section, the role of JDL level 5 is discussed.

5.13 JDL LEVEL 5 – HCI AND PROCESS IMPROVEMENTS

Level 5 of the JDL model is the Human Computer Interaction (HCI) level that provides a view into the system for the human operator (Schreiber-Ehle & Koch, 2012). The purpose of this level is to present the information obtained from the previous levels in

such a manner that the human operator obtains a clear representation of the current situation (Blasch & Plano, 2002). Level 5 of the JDL model is the final level, after which the process is re-evaluated and re-implemented. As discussed in Section 3.7, visualization is a complex endeavor but when implemented effectively, it has the potential to significantly enhance operator understanding of the current situation. Further discussion regarding level 5 implementation will be performed in the case studies presented in chapters 6 and 7. Additional discussion regarding the effectiveness of the visualization component will also be presented in Section 8.8.

The following section moves on to describe the experimental program architecture and to provide more information regarding the custom created cyber sensors.

5.14 EXPERIMENTAL SYSTEM ARCHITECTURE

The experimental system was designed for the web environment with the chosen language Visual C# for backend components and JavaScript and HTML 5 elements for the front end. The choice of programming language was a personal one, there are no significant benefits that any specific other language would have offered. The decision to design the application as a web application was mainly for future service offerings to both organizations and potentially the public at large. With a web application, the potential exists to access the information from anywhere and at any time, whereas with a desktop application, it would require some form of installation. The system was designed in phases with the initial phase focused on analyzing and visualizing the information available of the infrastructure in South Africa.

The experimental system developed made use of the data sources selected and discussed in Section 5.6. While all data sources selected relate to the attack surface as discussed in Section 3.2, the need for custom sensors was discussed in Section 5.6. The final experimental system is thus one system but can be logically grouped in different sections for ease of reference. Figure 5-8 presents a logical grouping of the experimental system based on the functions provided by the various components.

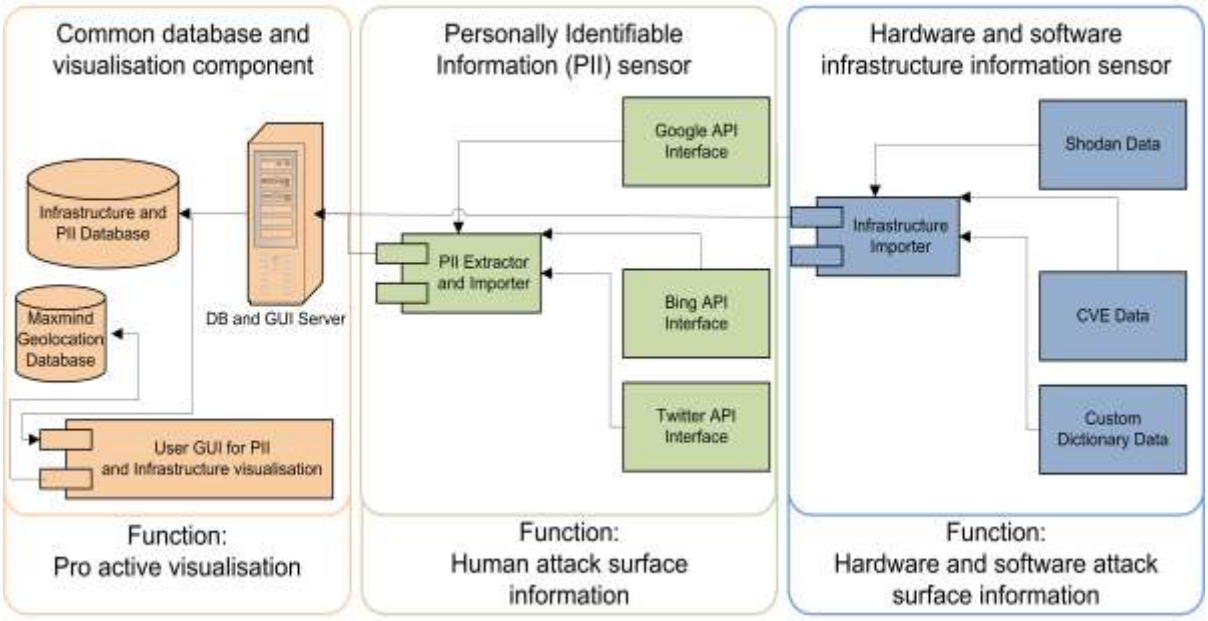

Figure 5-8: Experiment architecture logical grouping

Starting at the right of Figure 5-8 is the infrastructure information component that primarily makes use of the Shodan data. The infrastructure component is described in more detail in Section 5.14.1. The second logical grouping contains the custom PII detector, as described in Section5.14.2, that primarily provides information regarding the human component of the attack surface. The last logical grouping is the common database and visualization component to achieve pro active visualization of the vulnerabilities on a national level. The visualization component is discussed in a number of sections such as 5.13, 6.3, 0, and 8.10.1.3 to provide information regarding the role of visualization as well as the evaluation of the component.

5.14.1 INFRASTRUCTURE COMPONENT

Shodan has the ability to export large datasets either in XML[78], JSON or CVE but for effective fusion, faster access to data was required. Importing data into the experimental system for effective processing and fusion required a database to be designed and a file import utility to be created. The primary components of this section are illustrated in Figure 5-9. Datasets flow from their source to the importer section where it is processed and stored in the tables created for the infrastructure data.

[78] The XML export option was depreciated in favor of JSON

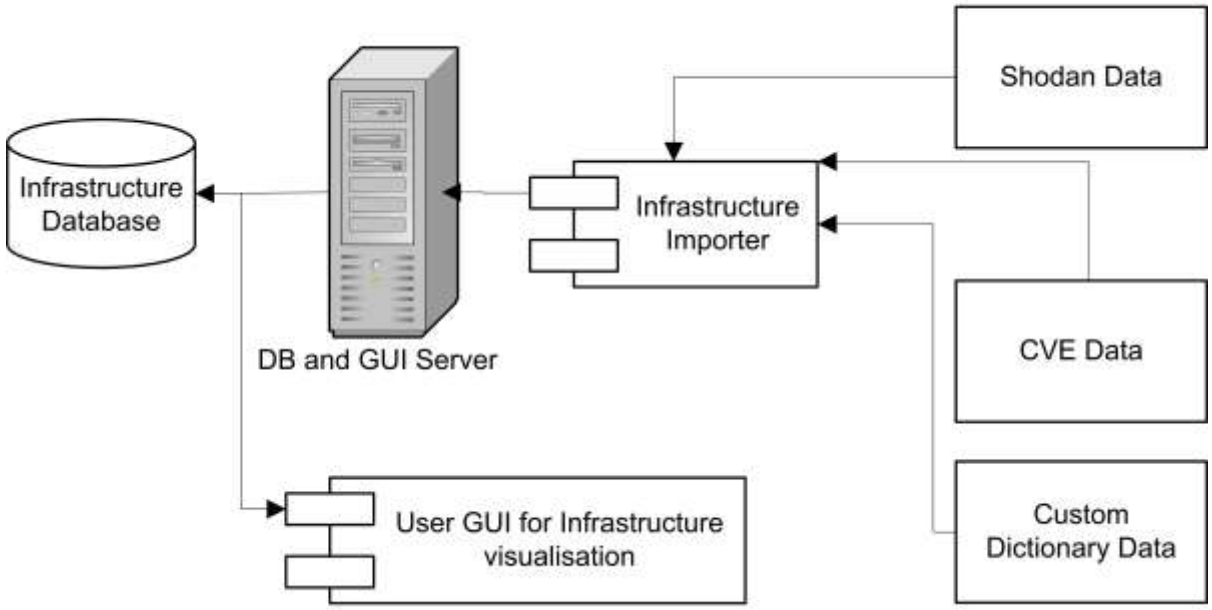

Figure 5-9: Infrastructure architecture

The database design was not only for Shodan data but had to incorporate both the CVE data lists and also custom dictionary datasets as described in Section 4.5.4. The result of the database design is available in Figure 5-10. Not all tables of the system are present in this diagram, only those with a specific focus on the infrastructure component of the experimental system.

One of the key features that a system such as this can provide is the ability to track changes in the environment over time based on the information that has been captured in the database. To achieve this, each dataset that is imported into the system is given a specific import number. While the visualisation component will only display the latest data captured at present, the potential is there track a historic view based on the older information sets. This will have significant value in future to determine what types of external initiatives resulted in the greatest impact from a managerial point of view.

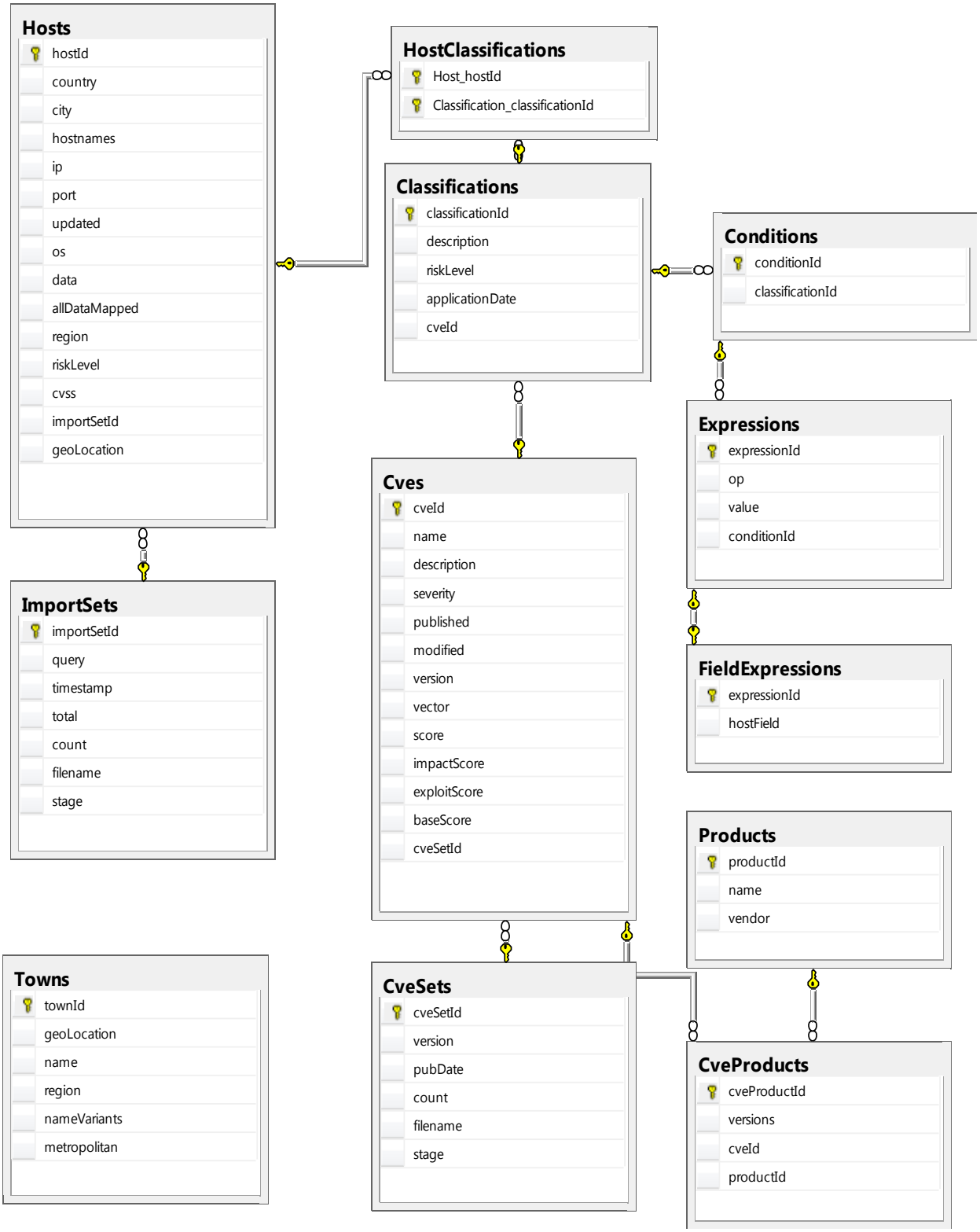

Figure 5-10: Database structure with relationships focused on hosts

5.14.2 PERSONAL INFORMATION EXTRACTOR

While it would be possible to actively scan all websites and IP ranges assigned to South Africa, obtaining an up-to-date list is unfeasible for entities outside of the domain administrator. This could also be considered illegal in the context of the ECT Act of 2002, since the precedent in South Africa has not yet been established in case law as to what level of scanning is acceptable. Further restrictions exist in the form of ISP fair use policies. Scanning infrastructure and spidering websites is almost always in breach of these policies. Over and above the previous limitations, several legislative regulations in the POPI Act of 2013 prohibit the processing of the obtained information. Care needs to be taken with the processing of the information found from the selected data sources to ensure that a system designed for detection of private information loss, does not end up in breach of regulations.

The experimental implementation was constructed by building on the visualization platform previously created for the infrastructure component discussed in Section 5.14.1. The experimental implementation was limited to finding the following types of PII for the duration of the experiment:

- ID number
- Land line telephone number
- Cell phone number
- Email address
- Credit card number
- Address
- Passwords (encrypted)

Data was specifically obtained from a variety of common files such as .txt, .sql, .doc, .docx, .xls, .xlsx, .csv and .pdf. While it is common for developers to create their own file structures, this experiment focused on the most commonly used files that had a higher probability of returning results. The architectural main components are depicted in Figure 5-11 and illustrate the links between the various components.

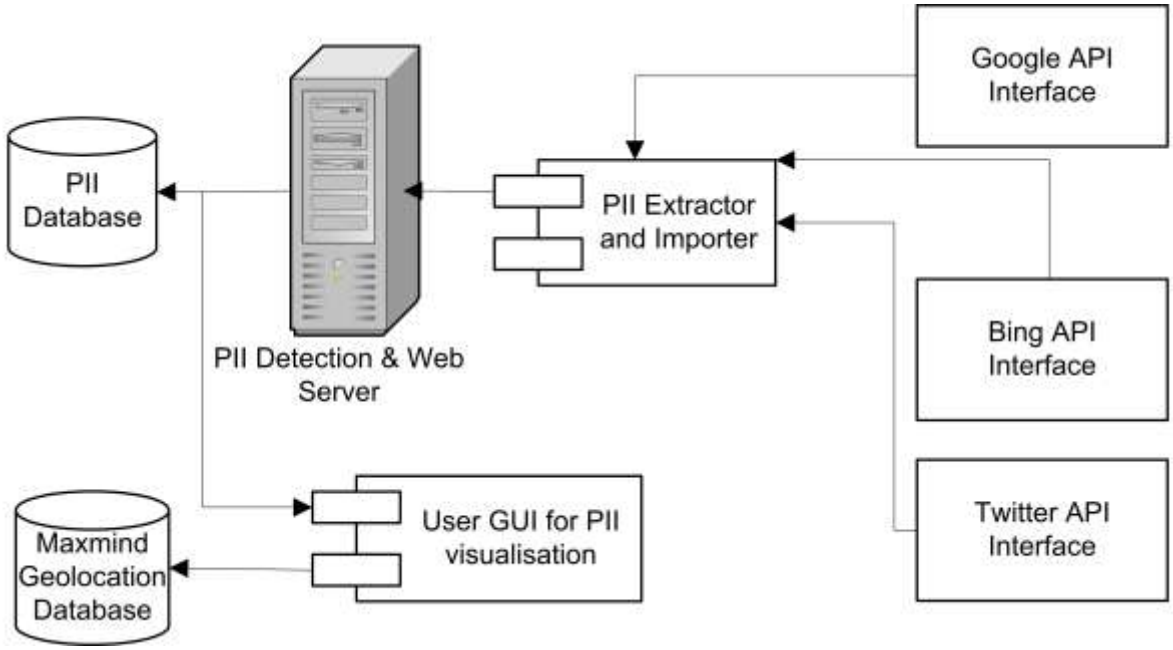

Figure 5-11: PII breach detection architecture

Data sources used in the experiment consisted of:

- Google Search API[79] - Provides access to Google's search API once a developer key is acquired. By utilizing keywords to search for, the search engine will return publicly available results that it has indexed.
- Twitter, Dump Monitor[80] - An experimental implementation that monitors a variety of paste sites effectively. These sites are often used to post hacked data and are a good source of information.
- Bing Search API[81] - Provides access to Microsoft Bing's search API once a developer key is acquired. Even though less keyword searches are available, there is still significant functionality available to detect PII breaches from this search engine.
- Maxmind Geographical IP location database[82] - The free version of the database was used in this experiment. Previous work has shown that this geographical IP location database has a reliable accuracy at the very least on national level (Poese et al., 2011).

Data sources for the system were free open access systems such as Google, Bing, DataBreach and a variety of pastebin sites such as those used in the Operation Sunrise

[79]https://developers.google.com/custom-search/json-api/v1/overview
[80] Twitter Profile - @dumpmon
[81] http://datamarket.azure.com/dataset/bing/search
[82] http://www.maxmind.com

data breach discussed in Section 4.4.8. Combined with the Maxmind commercial dataset already implemented in the first phase of the system, the visualization in Figure 7-5 was achieved. Personal information such as addresses and places of employment can be detected by using the OpenStreetMap API to evaluate if information is possibly related. To accommodate the new required information, the database had to be extended. The additional tables created to accommodate the obtained data are depicted in Figure 5-12.

Although commercial IP datasets have several limitations, an independent evaluation shows most datasets achieved a 98% accuracy in terms of country identified (Poese et al., 2011). This makes geolocation a reliable option to locate information stored on servers. While not always a requirement, the POPI Act of 2013 specifies in Section 72(i) that special provisions should apply to personal information stored internationally (South African Government Gazette, 2013). While the physical servers are hosted internationally, the domain name and IP address is key to attributing the data to South Africa, potentially binding it to established legislation. Data extraction was achieved with a variety of methods, most notably regular expressions. The data extracted from these sources were stored in the experimental system database, primarily in the tables depicted in Figure 5-12.

5.15 SUMMARY

The implemented design did not only focus on implementing a system in traditional system design architecture, but addressed the need for a formal data fusion model as well. The inclusion of the formal fusion model will allow for the implementation of more advanced data fusion techniques in future work at the various system levels. This will ensure that the efficiency of the experimental system can be increased to address the limitations identified in Section 8.10.2. With a modular design, the capability to add additional data sources such as those identified in chapter 4, is a real possibility.

Although not all levels of the JDL model are implemented in equal detail in the current experimental system, it does not detract from the potential benefit to be derived from such as system. Previous work has documented that not all levels of the JDL model have to be implemented for a system to contribute to increased situational awareness (Giacobe, 2013). Additional novel contributions of the system included the fusion of data leakage hosts detected on the South African Internet domain and previously unused filter mechanisms to detect malicious activity. This type of system has the potential to provide official responsible entities such as CSIRTs and privacy regulators with an opportunity to work reactively and potentially pro-actively at a low inset cost.

Figure 5-12: Database structure with relationships focused on personal information

Network security in the absence of host security is akin to hiring an armored car to deliver gold bars from someone living in a cardboard box to someone sleeping on a park bench.

Eugene Howard Spafford – Professor and computer security expert

6

Case study: South African national infrastructure

6.1 INTRODUCTION

The national cyber security policies described in Chapter 2 require governments to take responsibility for their respective Internet domains. In Chapter 3 the attack surface of such a national Internet domain was briefly discussed. This chapter will focus on examining the infrastructure and software available in the defined boundaries from open source intelligence data. As it is, the current experimental design will only provide a view of the devices directly connected to the Internet. This excludes any device behind a service, such as a proxy server that obfuscates the individual device. Thus, it should be clear that the number of devices that have access to the Internet will be far greater than the number reported by the current datasets. This is due to the fact that only a single machine needs to be directly connected to the Internet for all internal machines to make use of it via services such as Network Address Translation (NAT). The devices that connect systems to the Internet are typically one of the first contact points an attacker will have when conducting a remote attack. Gaining an understanding of the volume of these devices, their security profile and potential impact on a country is crucial to consider in national cyber security implementations. This chapter examines the Internet connected infrastructure devices for the South African domain from the data sources selected in Chapter 5.

6.2 DATA COLLECTION

Shodan data for the complete ZA domain was obtained at four different intervals from the period 31 February 2012 to 10 September 2013. The exact periods are listed in Table 6-1 along with the number of hosts available at the specific time and the cost associated with the data. Examples of data format and description of the relevant APIs utilized is available in Chapter 4 Section 4.4.2. Due to a lack of available research funding, a more

recent dataset is unfortunately not available. Since the September 2013 purchase, the Shodan system has been upgraded significantly and allows for comprehensive reports to be compiled. These reports do not provide details, only summary results, and will be used to supplement the information contained in this case study as required to reflect the most recent situational awareness available. The reports for example indicate that the number of hosts have reached a new high number of 1703366 on 2014-09-26. The latest dataset has not been purchased but is included in Table 6-1 in the last row to indicate the growth of discovered devices and the associated cost. Since the dataset is not currently available, the real number of hosts cannot be calculated.

Table 6-1: Shodan data purchased for the South African domain

Date	Number of hosts claimed	Number of hosts present	Number of unique hosts	Cost
2012-10-03	390128	5000	4062	$1 US
2013-02-11	536262	438550	289702	$99 US
2013-09-10	1251057	989385	693481	$154 US
2014-09-26	1703366	Undetermined	Undetermined	$427.5 US

The data listed in Table 6-1 column 1 shows the date the dataset was obtained on and column 2 shows the number of hosts that the Shodan service claim was present. Even though a full export was performed, the number of hosts received did not match the Shodan given numbers. Instead a lower number count of hosts available is given in column 3. Further reduction of the host number occurs in column 4 since Shodan lists each service as a unique record and for this experiment, a service is a attribute of a host. The merging of multiple services into properties of one host is performed at level 1 of the JDL model fusion process. Column 5 states the cost of the dataset purchased on the given date. All data obtained was imported into the experimental fusion system for processing in conjunction with the previously selected data sources. The reasons for selection of data sources to act as cyber sensors for the experimental fusion system is available and described in Section 5.6.

6.3 First visualization of acquired data and potential implications

The first attempt to visualize the Shodan data for the South African domain resulted in the image in Figure 6-1. The main focus of this visualization is to provide information regarding the distribution of devices in the national infrastructure. This potential

benefit of this type of visualization is to allow policy implementers a view of where assets are located in a geographic distribution. This is normally difficult to achieve since visibility into the cyber domain is typically limited as listed in Table 3-1 and described in Section 3.3. One of the requirements of effective policy implementation is to have the ability to take inventory of assets as described in Section 2.10 and cited as a reason why cyber security policy implementation is difficult. Visualization of the physical location of assets will assist policy makers the opportunity to focus their efforts not just based on social and anecdotal reports of device distribution but verifiable location distribution.

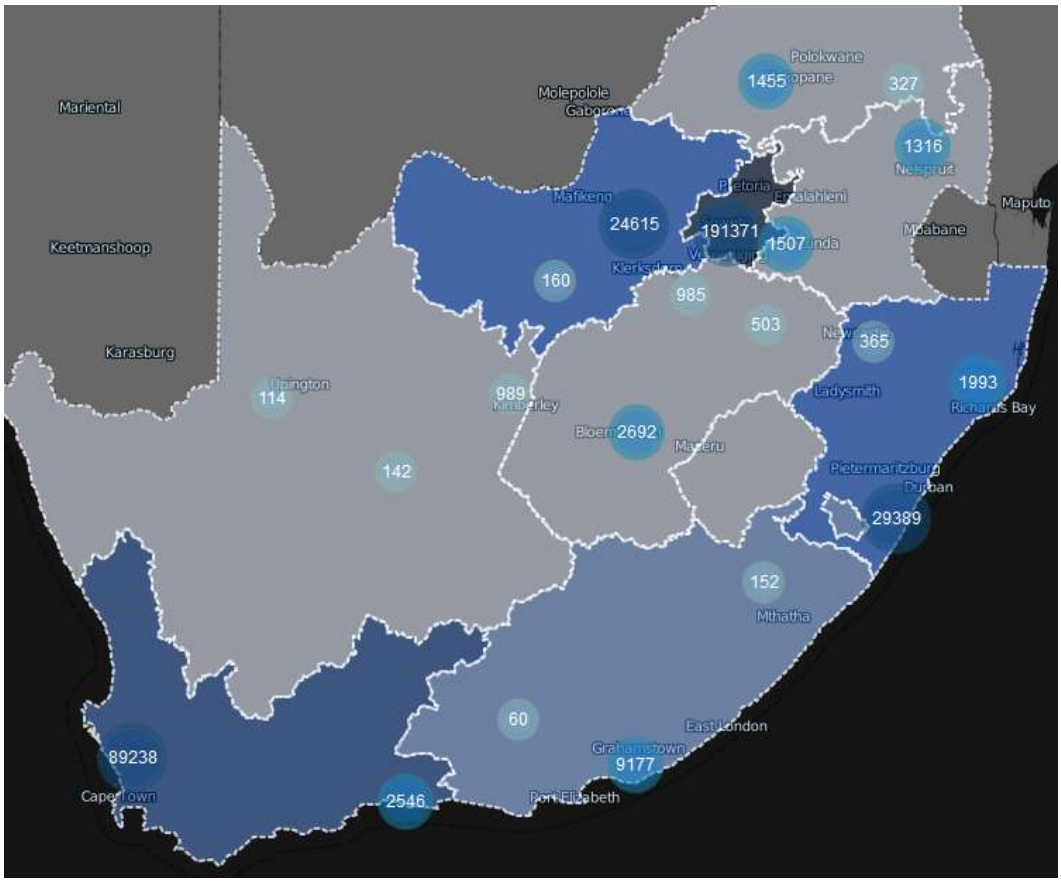

Figure 6-1: Clustering of Internet facing devices in South Africa 10th Sept 2013 dataset

While the information presented in Figure 6-1 is useful to present information regarding the infrastructure distribution in South Africa, summary data is hard to identify. It is still not an easy task to properly give accurate counts of the device distributions from the implemented visualization system. To this end a reporting component had to be created to allow for the summation of information as required. The results of the reporting component for the visualization of information in Figure 6-1 are available in Figure 6-2.

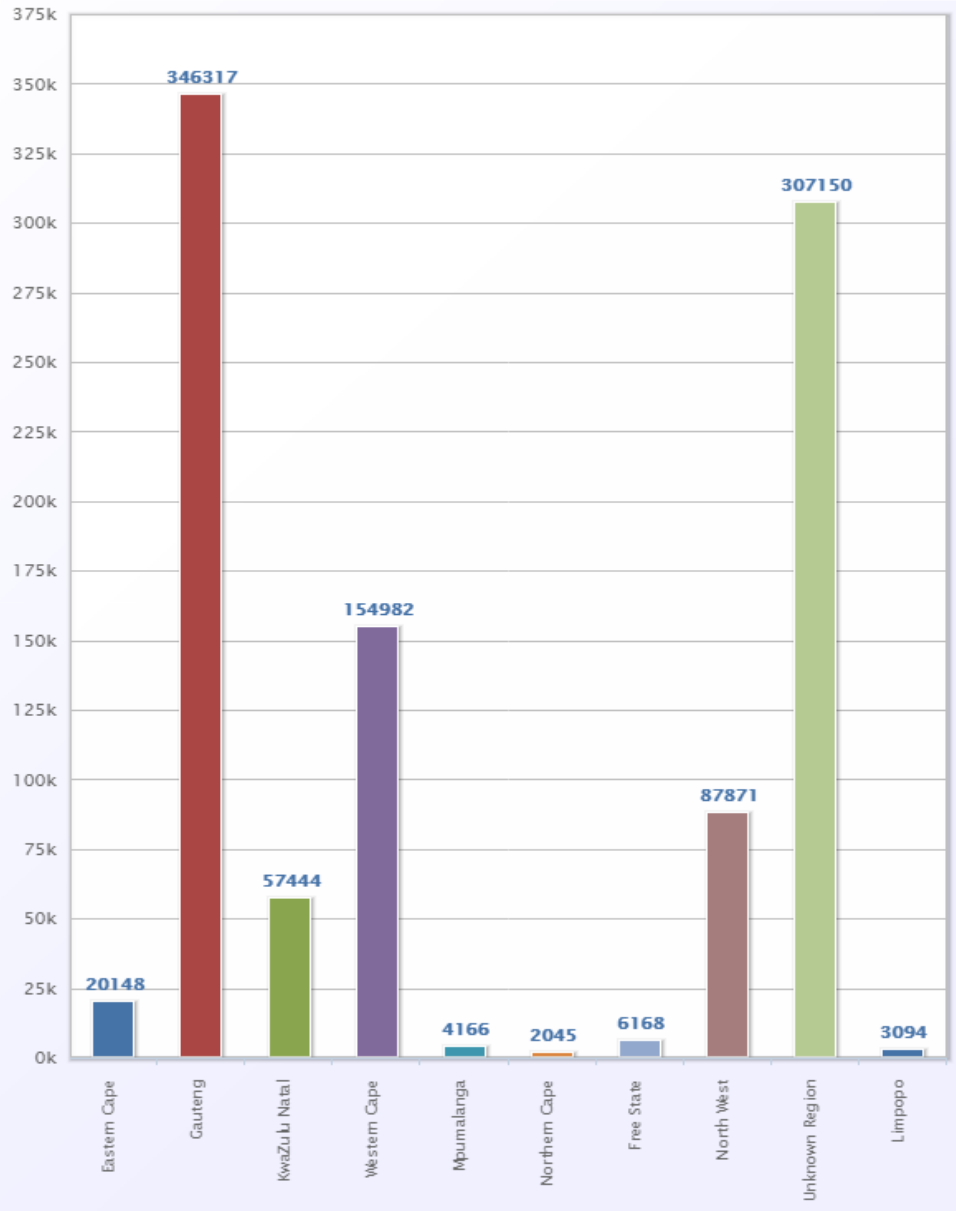

Figure 6-2: Internet facing devices grouped by South African province 10th Sept 2013 dataset

The data presented in Figure 6-2 provides clear and concise information regarding the distribution of devices in the South African domain in a simple bar-graph format. While the correlation of device distribution and population density is not explored in great detail in this study, it has been considered. Further opportunity for research can be established by considering the population distribution on a national level vs. device distribution on a national level, as shown in Table 6-2. The Shodan data set from 2013-09-10 was cross correlated with the publicly available information available regarding the South African national census[83] of 2011.

[83] http://beta2.statssa.gov.za

Table 6-2: Device and population distribution per province 2013-09-10

Province	Population	Devices	Ratio
Eastern Cape	6562053	20148	2187351:6716
Free-State	2745590	6168	1372795:3084
Gauteng	12272263	346317	12272263:346317
Kwazulu-Natal	10267300	57444	2566825:14361
Limpopo	5404868	3094	386062:221
Mpumalanga	4039939	4166	4039939:4166
Northern-Cape	1145861	2045	1145861:2045
North-West	3509953	87871	3509953:87871
Western-Cape	5822734	154982	2911367:77491
Unknown Region	-	307150	-
Summary	51770561	989385	-

A further breakdown of the information is possible by clustering the devices detected around approximate city centers. Since the list of available cities in a country is large, only the top ten cities according to device density will be listed. The list of cities with the most detected devices according to the 10th Sept 2013 dataset is available in Table 6-3.

Table 6-3: Top 10 cities for detected device location 2013-09-10 dataset

City	Device Count
Johannesburg	171866
Cape Town	108627
Potchefstroom	82005
Pretoria	80376
Durban	35128
Port Elizabeth	12317
Pietermaritzburg	8030
Benoni	7889
Bellville	7408
Boksburg	7092

This type of information may allude to the technological acceptance and reliance of different geographic regions in a nation. Alternatively it could also highlight how certain provinces have invested in technological infrastructure on a larger scale than other provinces or cities. As mentioned, these types of conclusions are out of the scope of this study; this section merely highlights the potential uses that a national fusion system could have. Further details such as the potentially most vulnerable province can be determined when Shodan data is combined with publicly available vulnerability database information. As described in Section 4.5.7, vulnerability databases are not perfect and should only serve to highlight potential vulnerability areas. Specialized equipment and dedicated security professionals should be deployed to verify the existence of the alluded vulnerabilities.

In the experimental fusion system, the NIST CVE database as discussed in Section 4.5.7 was utilized to identify potential vulnerabilities. The data containing the relevant extracted information is presented in Table 6-4.

Table 6-4: Vulnerability distribution per province 2013-09-10 dataset

Province	Population	Devices	Potential Vulnerability Count
Eastern Cape	6562053	20148	229202
Free-State	2745590	6168	70218
Gauteng	12272263	346317	5421291
Kwazulu-Natal	10267300	57444	723209
Limpopo	5404868	3094	24084
Mpumalanga	4039939	4166	50404
Northern-Cape	1145861	2045	11077
North-West	3509953	87871	135226
Western-Cape	5822734	154982	2174833
Unknown Region	-	307150	3283520

The results obtained for the calculation in the example experiment returned a total of 78463 vulnerable devices with an average CVE score of 5.91. The CVSS scoring system was discussed in Section 4.5.7 and provides a score out of 10 with 1 as the least critical and 10 as the most critical. Remarkably the average score of 5.91 is a close match to an

independent study discussed in Section 2.7, that concluded that the average CVSS score of online content management systems for South Africa is 5.4 (van Rooyen, 2014).

A detailed breakdown of CVSS score distribution is available in Table 6-5. It should be noted that other vulnerabilities such as physical security weaknesses is beyond the scope of this experiment and will thus not be reflected in the results of this metric. This reduces the accuracy of the current measurement but since a typical PDCA process is prescribed by the cyber security policy implementation framework for security implementations, additional variables can be incorporated in future approaches. The generic cyber security policy implementation framework was discussed in Section 2.8.

Table 6-5: Breakdown of vulnerable hosts by severity 2013-09-10 dataset

CVSS score	2	3	4	5	6	7	8	9	10
Number of Hosts affected	20540	413	23565	4667	419	18929	389	1553	7988

The data in Table 6-5 has interesting properties considering the large number of hosts applicable to the study. A histogram of the distribution of vulnerabilities is available in Figure 6-3 for ease of reference. The three outliers are CVSS scores 2, 4 and 7, that account for 80.3% of all vulnerable hosts. Considering the significant difference required to calculate these scores it points to the potential that a small collection of CVE numbers is responsible for a large number of vulnerabilities.

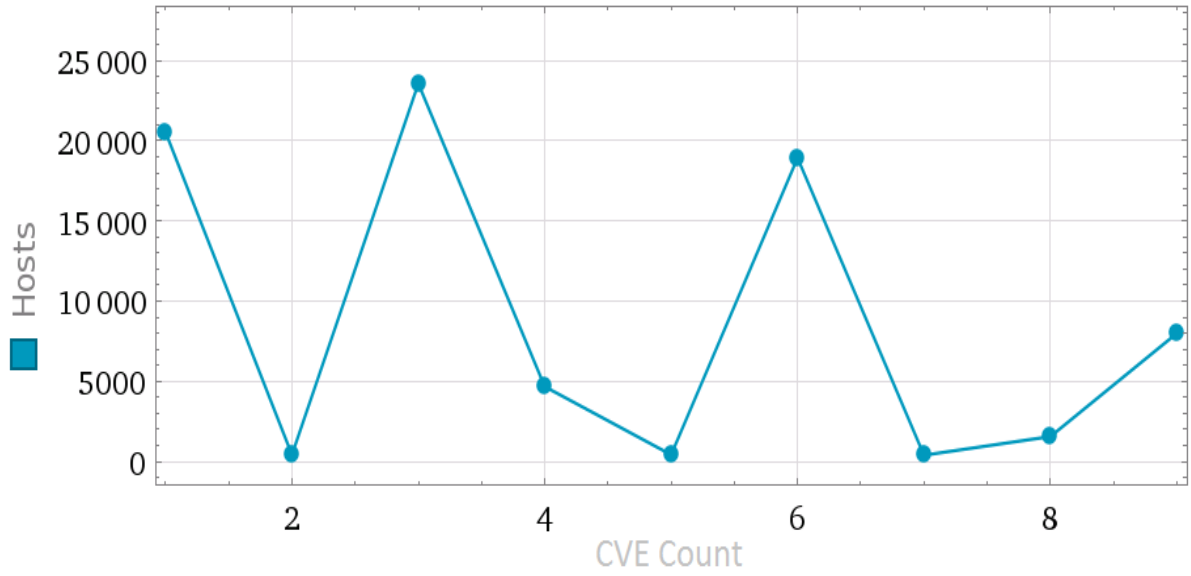

Figure 6-3: Host and CVSS distribution 2013-09-10 dataset

By examining the data, policy implementers will have the opportunity to allocate resources to where it is most required. Not all provinces in a country have the same economic strength and this type of data will allow priorities for cyber security implementation to be set, at least based on a vulnerable device level. Further breakdown of the information can be used to set information security training requirements for administrators and first responders. By performing a query on the experiment dataset for all software packages that contains vulnerabilities, a list of 699 different software packages were returned. While this list is too long to include, it is possible to group the software packages by vendor. The top ten products are listed in Table 6-6 with the corresponding number of products identified that suffer from vulnerabilities.

Table 6-6: Vendor responsible for vulnerabilities 2013-09-10 dataset

Vendor	Number of products identified
HP	1335
CISCO	851
IBM	435
Microsoft	317
Oracle	204
Hitachi	175
Sun	165
Symantec	165
CA	151
Joomla	145

Obtaining information regarding the hardware and software platforms most utilized in a specific country has several benefits. A key requirement of at least four current cyber security strategies is testing of deployed government off the shelf infrastructure (Luiijf et al., 2013). With the information obtained, priorities can be set and cost can be contained since the product range most used is known. Testing device and software platforms might seem trivial but should not be discarded lightly. Research has shown that different devices handle different traffic loads in a different ways. Incorrect packet formatting can result in devices restarting, simply dropping packets or to simply stop

responding at all (Morris et al., 2011). This has significant implications for national security and if verification services are to be implemented on a national level, training for specific vendor devices can speed up the process.

6.4 PROVIDING MORE DETAILS

Good visualization practice is to provide a summary overview and allow for details on demand to be obtained, as discussed in Section 5.13. With this in mind, the experimental system provides the ability to zoom into a desired location and to obtain further details regarding the area under investigation. When zooming into the specified region, clusters of devices breaks down into smaller clusters, as shown in Figure 6-4.

The provision to allow for zooming into greater detail allow for additional features to be added as they become relevant to device or area under investigation. Further discussion of the details relevant to devices located on the Internet will be provided in the following section.

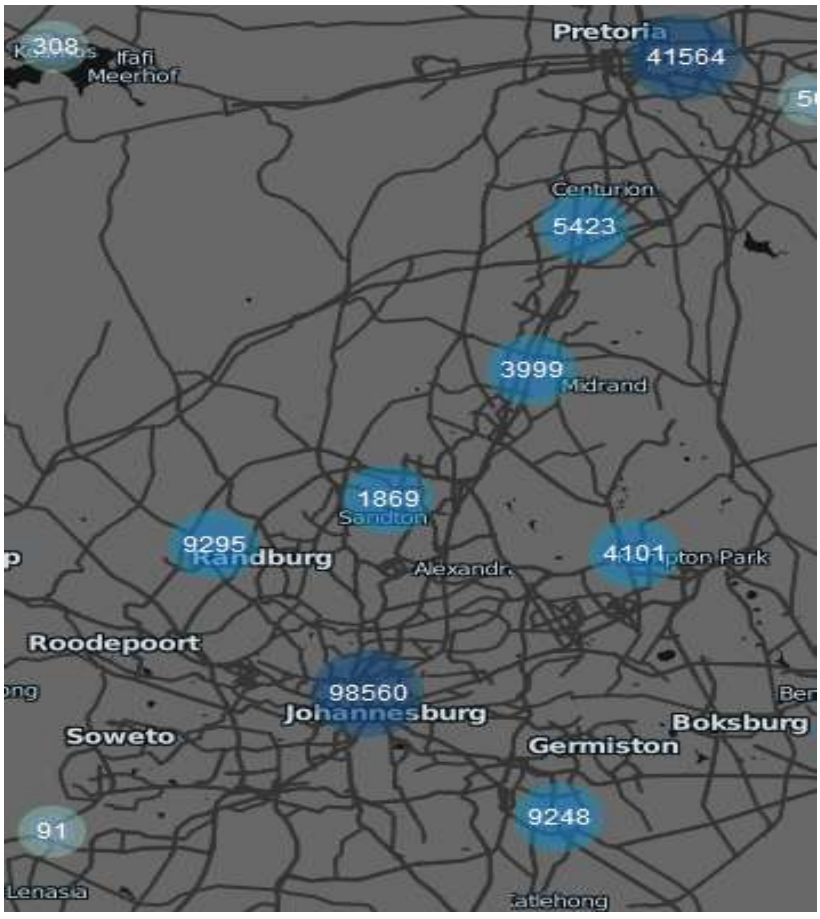

Figure 6-4: Detected Internet facing devices in a provincial region 2013-06-15 dataset

6.5 CASE STUDY A: LOCATING A HOST WITH A CRITICAL VULNERABILITY

As an example a high level view of Gauteng is presented in Figure 6-5. A heat map was generated based on the risk profile of the available hosts in the region. Matching is achieved by evaluating the host description against the various CVEs available as described in layer 0 of the JDL model in Section 5.8. The heat map color scheme can be implemented in various ways, but in this experiment the common method of increasing color intensity to match severity is used. Hosts with a critical CVE will be assigned a red color while hosts with lower severity scores will be assigned less intense colors. In this instance yellow for intermediate scoring hosts and teal for low scoring hosts were used.

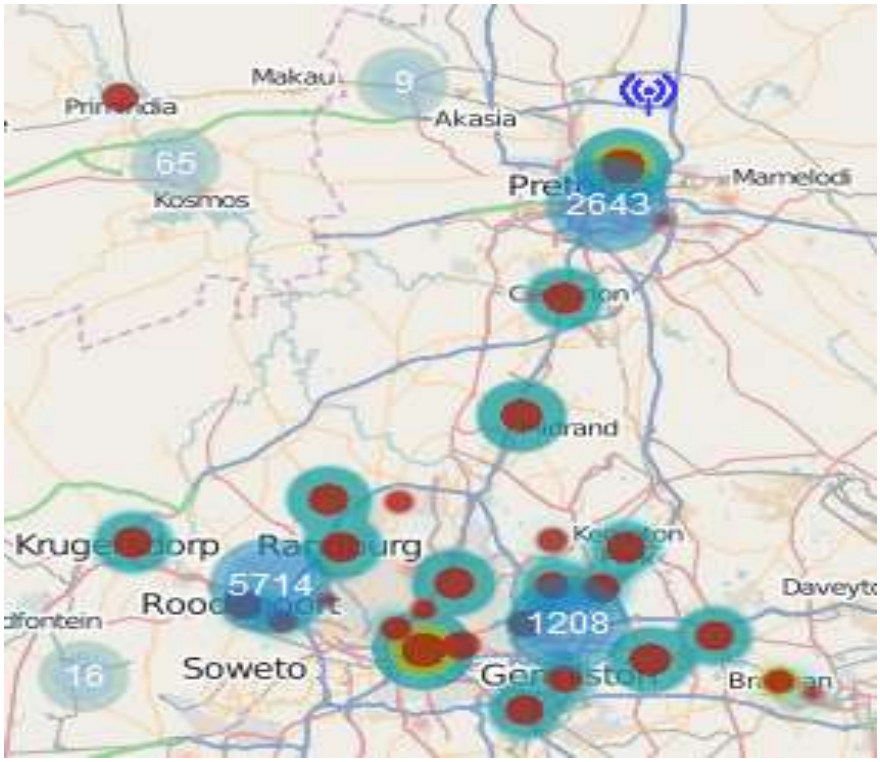

Figure 6-5: Heat map implementation of CVEs 2013-06-15 dataset

While heat maps work well when the zoom level is at a low enough level, as soon as specific details were required it became cumbersome. Instead the color scheme was retained but applied on individual hosts as soon as the level of zoom was sufficient to start identifying individual hosts. This is demonstrated in Figure 6-6 where a host with a critical vulnerability was identified.

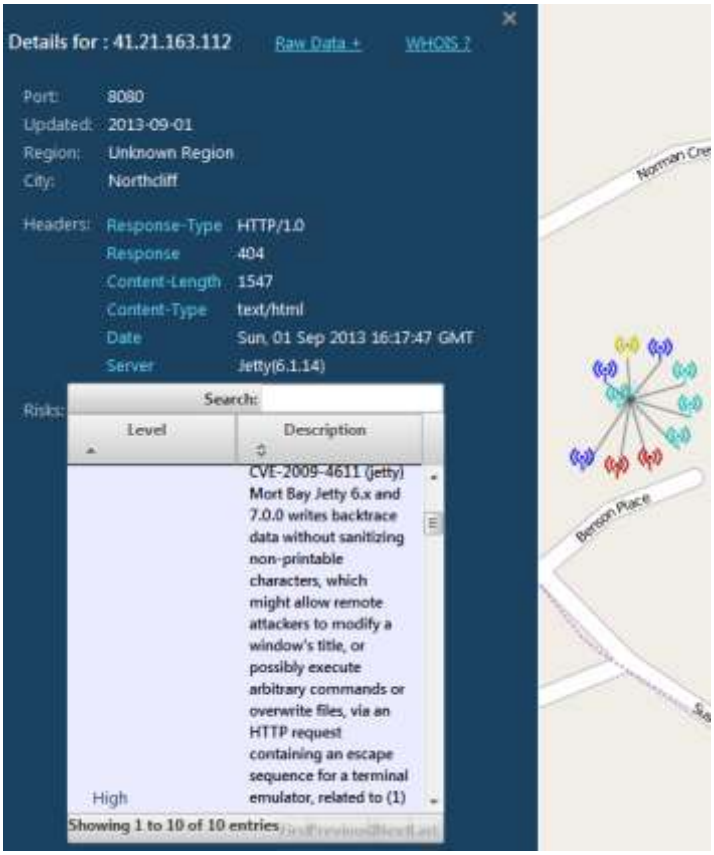

Figure 6-6: Individual selection of a host with associated detail panel 2013-06-15 dataset

In this example, the only manner to negate the vulnerability detected on this devices is to update the server software. This requires the co-operation of the relevant ISP to locate the owner of the IP address. Fortunately, the WHOIS lookup service is widely implemented and this provides contact information for the vulnerability. If information returned from WHOIS is not for the responsible individual, at least the responsible registrar or ISP will be identified.

6.6 CASE STUDY B: LOCATING HACKER ACTIVITY

Detection of hacker activity is fairly difficult to accomplish if the disruption to the system under attack is kept to a minimum. Should no resources be disrupted that are required to function, the intrusion might not be discovered for a significant amount of time. In the experimental fusion system, the available infrastructure dataset was parsed and processed with natural language filters to search for words similar to those contained in a generated leet speak dictionary (as introduced in Section 4.5.4). Several instances were found but by far the most interesting was the banner depicted in Figure 6-7. The banner information contained a clear indication that there might have been illegal access gained on the device.

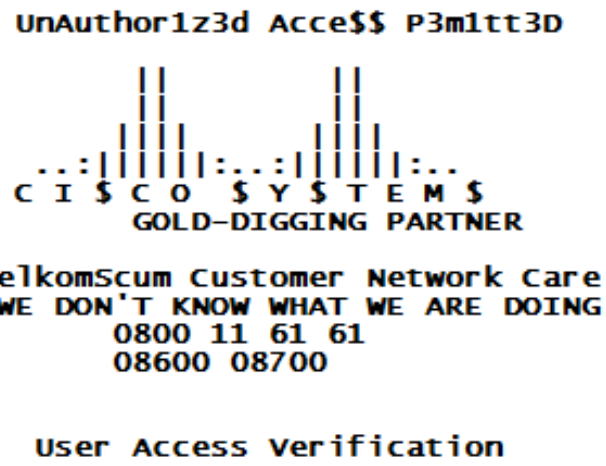

Figure 6-7: Example of Leet speak detected in the South African Shodan dataset

With the use of device banner information, hostname, WHOIS lookups and email communication, the administrators were notified. While Leet speak is only an indicator, communication with the administrators confirmed that a breach did indeed occur. In this instance the administrators were part of a vast organization and could not immediately pinpoint the location of the device in their network. Locating the device turned out to be quite troublesome since equipment is constantly moving between departments. Through the use of the available geolocation information, an approximate region to investigate was identified and the issue was resolved. Since the device in question was chiefly an Internet gateway device, it was not always scrutinized by administrators and it is uncertain how long ago the devices were breached. This type of incident clearly highlights the benefits of implementing a monitoring system to regularly check local device configurations from the outside. Due to confidentiality reasons, the responsible organizations were not named. The banner is presented in original form and it should be noted that the telecommunication company Telkom was not the affected party.

6.7 CASE STUDY C: ROUTERS WITH DOCUMENTED VULNERABILITIES

South Africa has seen an increase in connectivity from both individuals and businesses with year-on-year double digit growth rates for Internet penetration (Goldstuck, 2012). This uptake is not just from one segment of the economy, all segments increasingly make use of ICT regardless of their size. A significant uptake of ICT even in small to medium enterprises (SME) has been documented (Adeniran & Johnston, 2014). While the increased use of the Internet is good for the South African economy since it has the potential to lower the cost of doing business and increase education of individuals, it also

creates additional risk. Exposing systems to the Internet without proper security implementations can have severe consequences for owners. Enterprises such as SMEs that have a limited budget for security operations are particularly vulnerable to these types of attacks and by all accounts, the attacks on SMEs are increasing worldwide (Kyobe et al., 2012; Hayes & Bodhani, 2013; Lewis et al., 2014). Individuals are also placed at risk if they are not made aware of the current state of vulnerabilities that could affect them.

This embedded case study will examine an often overlooked attack vector that has received increased attention in the past few years and affects all sectors of the economy. The Small Office Home Office (SOHO) router is often installed by a telecommunication company installer and once installation is completed, left unchecked and untouched for extended periods. Antivirus and application firewalls do not monitor the router and often the device does not possess the ability to update firmware versions remotely even if an update is available. The requirement to keep device firmware updated is not typically made clear to device owners and it was found that router manuals place very little emphasis on security in general (Szewczyk, 2013). Consider that routers are typically used as gateways to connect to the Internet and are often the first point of contact into a network. This presents the router as an attractive target for attackers. Should an attacker gain access to the router, at the very least they would have the potential to redirect web traffic to a location of their choice.

The redirection of traffic is exactly what happened in a previously documented incident where more than 4.5 million routers were compromised (Assolini, 2012). Hackers compromised routers in the Brazil region and altered the primary DNS entry to a address of a DNS server under their control. At periodic intervals the traffic would be redirected to malicious domains with the aim to gain access to banking details from the owners of the compromised devices. What makes this attack especially troubling is the fact that the owner of the device had almost no chance not to be affected by the attack. Even if the owner selected a strong password, the vulnerability was a Cross Side Request Forgery (CSRF) that negated the need for a password.

In another instance of mass router compromise, flaws found in ASUS firmware allowed attackers to access any storage devices directly connected to the router (Goodin, 2014). The attack could be considered non-malicious by some since the only indicator of compromise was a text file created on the affected storage device. The created text file merely contained a warning that the attack was possible and disclosed the location of

other vulnerable device's IP addresses. The disclosure was hosted on Pastebin[84] and contained over 30000 affected IPv4 device addresses. The lack of a severe attack in this instance does not negate the severity of the vulnerability. The vulnerability provided access to files that users considered safe from external entities. As such, any amount of personal information, potential intellectual property or other confidential information could have been accessed. Even more troubling was the fact that the vulnerability was reported[85] to the manufacturer nearly a year before the attack. The quoted response from the manufacturer was that the vulnerability reported "*was not an issue*".

The above examples of router compromise indicates that the threat is very real with a significant potential for exploits that can cause economic loss. The loss will not be contained to individuals but has the potential to affect any segment of economy participants such as small to medium enterprises, important to the South African economy. In the example of the Brazil attack, the devices were obtained from various ISPs as part of a package for internet service. South Africa follows a similar model where ISPs typically provide the router required to connect to the Internet as part of a contract agreement. By applying published research on vulnerable devices, it should be possible to gain at least an estimate of the devices affected by disclosed vulnerabilities still in service. This case study considered the research performed by Vanderbeken (2014) and Independent Security Evaluators (2013b) as the primary sources of recent vulnerable router information. Both sources contain information regarding the specific router model and firmware versions that are affected. In addition, both sources describe vulnerabilities that are not considered difficult to exploit and as such, presents the highest risk.

Finding the devices in the available dataset requires some form of unique identification since the dataset contained a large number of records. Most device manufacturers surveyed in this embedded case study included the device make and model in the banner information of the router. This allows a search to be performed on the router model by making use of the model number of the route where it was provided. In instances where the model number is not available in the header, it becomes unfeasible to obtain a indicator relating to the model number. Belkin routers that also have documented vulnerabilities in the N300 and N900 models, are not easy to detect (Independent Security Evaluators, 2013a). Since the Belkin routers only return generic

[84] http://pastebin.com/ASfYTWgw
[85] http://www.securityfocus.com/archive/1/526942

brand information and not specific model version numbers, the experiment is unable to estimate the availability of these devices without active testing. The number of devices detected by type in the search result is listed in Table 6-7 with the type of vulnerability listed where applicable.

Table 6-7: Number of routers with known vulnerabilities 2013-09-10 dataset

Router	Buffer Overflow	Samba Symlink	Race Condition	Web Attacks	Backdoor	Improper File Permissions	Count
ASUS RT-AC66U	X	X				X	18
ASUS RT-N56U		X				X	31
D-LINK DIR-865L		X	X	X	X	X	0
Linksys EA6500		X		X		X	0
Linksys WAG120N					X		30
Linksys WAG160N					X		3
Linksys WAG200G					X		18
Linksys WAG320N					X		1
Linksys WAG54G2					X		3
Linksys WAG54GS					X		5
Linksys WRT300N					X		0
Netgear WNDR4700		X			X	X	0
Netgear WNR3500		X			X	X	23
Netgear DG834					X		2650
Netgear DGN1000					X		5309
Netgear DGN1000B					X		0
Netgear DGN2000					X		481

Router	Buffer Overflow	Samba Symlink	Race Condition	Web Attacks	Backdoor	Improper File Permissions	Count
Netgear DGN2000B					X		0
Netgear DGN3500					X		200
Netgear DGND3300					X		1
Netgear DM111					X		6
Netgear JNR3210					X		0
TP LINK TL-1043ND		X	X	X			0
TP LINK TL-WDR4300		X		X		X	0
Trendnet TEW-812DRU	X			X	X		0

The identification of incorrectly configured router devices is also possible by examining the default message that appears when a router is configured for the first time. As an example, the popular Cisco routers' initial configuration provides a privileged account to allow the user the opportunity to configure the device for its intended role. The message received when connecting to the router clearly states that the account is purely meant to be accessible initially and should be password protected as soon as possible. The initial level 15 account provided by the Cisco IOS is a privileged account that provides full control over the device and is normally password protected (Cui, Kataria & Stolfo, 2013). Since the CISCO device reports a distinctive message upon contacting the device, it is possible to locate incorrectly configured devices in a similar fashion as detecting potentially vulnerable routers discussed previously. The results for the search term "level 15" in the experimental system returns 302 distinct devices and further verification could be deemed illegal under current South African legislation.

The work considered for this embedded case study is by no means a comprehensive account of all vulnerabilities documented for SOHO routers. Notable vulnerabilities that affects large groups of devices such as Universal Plug and Play (UPnP) should also be considered in future experiments (H. Moore, 2013). At present the dataset does not

contain sufficient information regarding the ports that UPnP operates on, and as such, was not discussed. The vulnerabilities described in this section is also not limited to routers specifically. Various other types of devices such as Building Control Management devices could also be affected by these types of vulnerabilities (Bonkoski, Bielawski & Halderman, 2013).

6.8 SUMMARY

While currently relying almost exclusively on a variety of external data sources, the experimental system implemented has shown great potential to visualize information security information regarding infrastructure coherently. Visualization techniques such as graphing, heat maps, clustering and layering were effectively used to present an easy to navigate system. Combined with an underlying data fusion engine, the potential to obtain information regarding the state of a nation's information security has been demonstrated. While the results definitely contain a degree of error and omission, the argument can still be made that the experimental system has significant benefits. A system such as this highlights the need for more research to be performed to allow accurate scan results, reliable vulnerability reporting and overcome owner communication difficulties. In addition the visualization of fusion process results allows at least for an adequate understanding of device type, distribution and with enough time, a method to determine if the amount of devices vulnerable is increasing or decreasing.

This chapter examined the infrastructure present in a country and the type of information that can be derived from the selected data sources in the fusion process. The next chapter makes use of the same fusion and visualisation system presented in this chapter but shifts the focus from infrastructure to the human component of the attack surface. Since no adequate data source was found to provide information regarding the human aspect of the national attack surface (discussed in Section 3.2), one had to be created. The case study in the next chapter presents the results obtained from the created sensor based on the architecture presented in Section 5.14.

If someone steals your password, you can change it. But if someone steals your thumbprint, you can't get a new thumb. The failure modes are very different.

Bruce Schneider – Cryptographer, security and privacy expert

7

Case Study: The automated detection of PII in South Africa

7.1 INTRODUCTION

In the previous chapter, devices that allow communication to occur on the Internet were examined. Without these devices, communication will not occur and since the Internet exposed devices are potentially the first contact point for attackers, obtaining information regarding their security profile is crucial. There is however more than one way to gain access to systems when the attack surface of a organization or even a nation is examined. People form an integral part of today's information processing operations and can be exploited just as easily as the Internet connected infrastructure. With the frequency and scale of data breaches growing to unimagined proportions, the need to protect PII is evident. This chapter will provide a summary introduction of the importance of PII and the current limitation available for detecting exposure of this information. Once the reader is familiar with the need for PII protection, the results of a case study conducted for the protection of South African PII will be discussed.

7.2 PERSONALLY IDENTIFIABLE INFORMATION BACKGROUND

PII is currently widely leaked from a variety of sources such as hackers, employees and incorrect infrastructure configurations. Guilt for the leakage cannot always be attributed to negligence by the business owner since there are legitimate business reasons to share data with third party vendors (Papadimitriou & Garcia-Molina, 2011). While the numbers vary for the amount of records leaked, examining some of the documented and acknowledged breaches that occurred gives an indication of the scale of the problem. Target in the USA leaked well over 10 million customers records in 2013 and Sony leaked 77 million customer records in 2011. While South Africa has not seen leaked PII numbers of that scale, the hack from team GhostShell in Operation Daybreak revealed in excess of 70 000 full detail records (Swart et al., 2013). In a recent study by

the Ponemon Institute (2013), they conclude that the average number of unique data records leaked during an incident is between 18237 and 34249.

Some of the primary reasons that PII is so important to protect are highlighted by the following research:

- Spam email combined with even as little as one piece of PII has a success rate of well over 70% in phishing attacks. This is in stark contrast to the 3% effectiveness normally obtained by spam campaigns (Sheng, Holbrook, Kumaraguru, Cranor & Downs, 2010).
- It is estimated that the PII loss cost companies well over 80 million US dollars in 2013 (Ponemon Institute, 2013). While traditional loss reports have been discredited due to the collection method of the report, the Ponemon work is touted as free of this error. The data is based on actual payouts from the insurance provider and not based on customer survey results.
- Privacy is often abused as a result of PII leakage in various forms such as identity theft or unauthorized transacting (Krishnamurthy, 2010).
- As interaction on the Internet increases, so does the chance for abuse if sufficient protection is not put in place.

In South Africa there are currently several pieces of legislation set in place to protect personal information such as the ECT Act of 2002 (South African Government Gazette, 2003) and more specifically the POPI Act of 2013 (South African Government Gazette, 2013). These acts have placed South Africa well on par with other countries with well established privacy legislation such as the UK. It has also been proven that just the implementation of data breach laws has the possibility to reduce losses due to data leakage by as much as 6.1% (Romanosky, Telang & Acquisti, 2011). This is despite the fact that current enforcement of said legislation happens primarily on a reactive basis with no clear guidelines on a pro-active approach.

A reactive approach is not a uniquely South African problem, it is currently estimated that well over 70% of PII breaches are reported by third parties globally. Even on a policy level organizations tend to have a reactive approach, changing their corporate tactics only if public outcry occurs (Culnan & Bies, 2003). While it is distressing that curators of personal information have to be told when the data is not under their control anymore, a far worse factor is the amount of time it takes before incident discovery. The timeline for recorded breach discovery is anything between immediate discovery and

several years. The vast majority of breaches take several months to discover and instead of this trend moving down, it is increasing at an alarming rate, as shown in Figure 7-1 (Verizon, 2013).

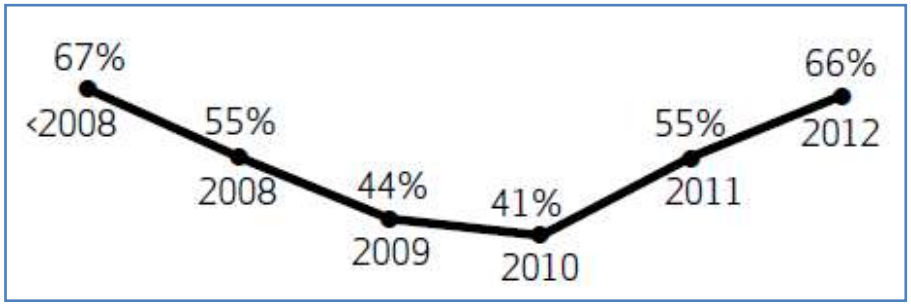

Figure 7-1: Percentage of breaches taking more than a month to be discovered (Verizon, 2013)

Current software tools to address this problem are available but they function primarily on a individual and corporate network level (Hart, Manadhata & Johnson, 2011; Shabtai, Elovici & Rokach, 2012). Work performed by Sokolova, Emam, Arbuckle, Neri, Rose and Jonker (2012) has taken a step in the right direction but their focus was primarily Personal Health Information (PHI) located on the public peer-to-peer networks. There are still a huge number of untapped sources that could shed light on the extent of PII leakage and allow governments to effectively enforce legislation. In this experiment, a subset of the available data sources discussed in Chapter 4 applicable to personal information will be examined. The majority of data is provided by the PII component of the experimental system, discussed in Section 5.14.2.

7.3 DATA COLLECTION

Once the experimental system was activated, an initial surge of potential PII data was obtained from public data sources. After the initial volume of detected items were processed, the detection of potential new items dropped down significantly as shown in Figure 7-2. The sudden drop in new results after the initial detection phase can be explained by examining the manner in which public search engines currently work. Typing in the same request in a search engine is not guaranteed to deliver the same page returned in every instance. Over time, the search engine operators make use of a variety of metrics to determine the most used page for a certain topic. The metrics that determine which page is returned first, are also not set in stone. Constant adaptation to the algorithms that determine page ranking is performed. This type of event might explain the sudden rise in detected information near the end of June 2014, but it is currently not possible to verify this assumption.

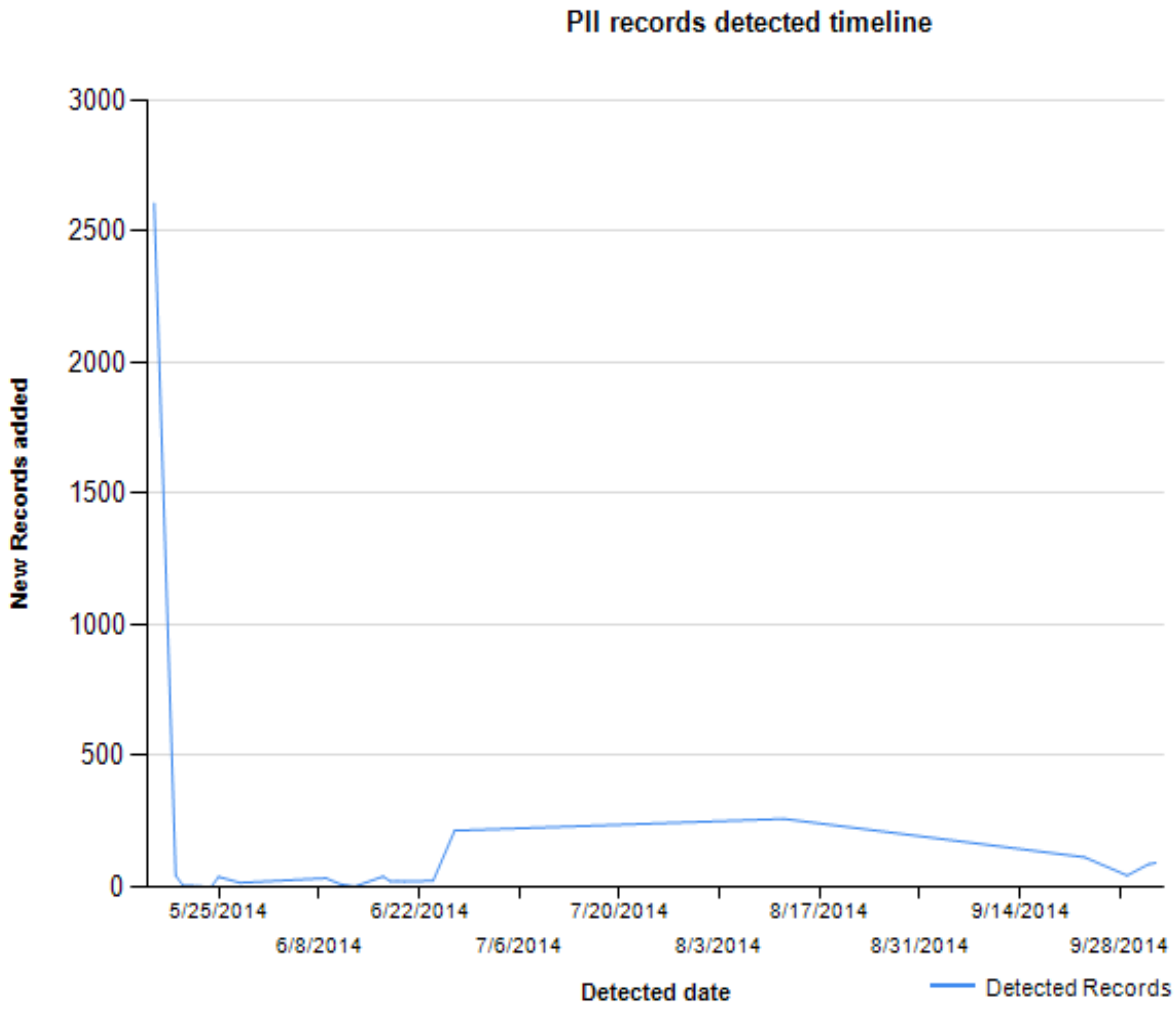

Figure 7-2: Automated PII data collection timeline

As a reminder, consider that the experimental system only examined URLs that contained files, as discussed in Section 5.14.1. No HTML scraping was performed and should this have been included, the number of detections would have been significantly higher. Several instances can be documented where the information was available in HTML format but not in any of the selected file formats.

To validate the claim that the sudden drop in new results could be attributed to the manner in which public search engines work, a deviation of normal experimental procedure was implemented. Near the end of the analysis period 5000 extra queries were purchased from both the Google and Bing search engines to examine the effect this would have on the data collection results. An immediate increase in the number of results available for investigation was recorded, thereby confirming the initial claim.

7.4 DATA EXTRACTION TECHNIQUES

Data obtained with the collection module had to be processed for the various categories of PII described in Section 5.14.2. Work in this regard was first started with the Operation Sunrise date breach as described in Section 4.4.8 to determine the results of the breach as listed in Table 4-9. To effectively analyze the leaked data, a custom system had to be designed to extract PII from the various unstructured data sources the data had been dumped with. In this instance, the location used was a series of Pastebin alternative sites that operate on a similar principle as the original Pastebin[86]. These sites provide any user with the ability to instantly share information anonymously with anyone connected to the Internet. These types of sites are popular data breach disclosure locations and Operation Sunrise was no exception.

At first glance it seems like a trivial task to extract all information from the data made available on the various paste bin sites. As previously documented, this type of exercise is far from trivial if any degree of accuracy is a requirement. One of the primary factors complicating PII data extraction is the fact that data is often sourced from numerous different companies. Each company represents data in their own unique manner and this results in no single structure that records are presented in. Furthermore, making use of information extraction techniques such as regex is a good manner to pattern match data. Unfortunately, regex will also match information that might not be correct. This requires that each dataset that is extracted needs to be validated for accuracy before it could be accepted as a true leaked record.

The application depicted in Figure 7-3 provides users with the ability to select the various files required for potential PII leakage analysis. Later functionality included the option to examine the data located at a web server since it is a time consuming process to download and store all detected PII available from the various Pastebin sites. Once the files required for processing are selected, processing commences and extracts information such as South African ID numbers, telephone numbers, cell phone numbers and credit card numbers. The data presented in Figure 7-3 and Figure 7-4 was partially grayed to protect the parties affected by the breach.

[86] http://pastebin.com

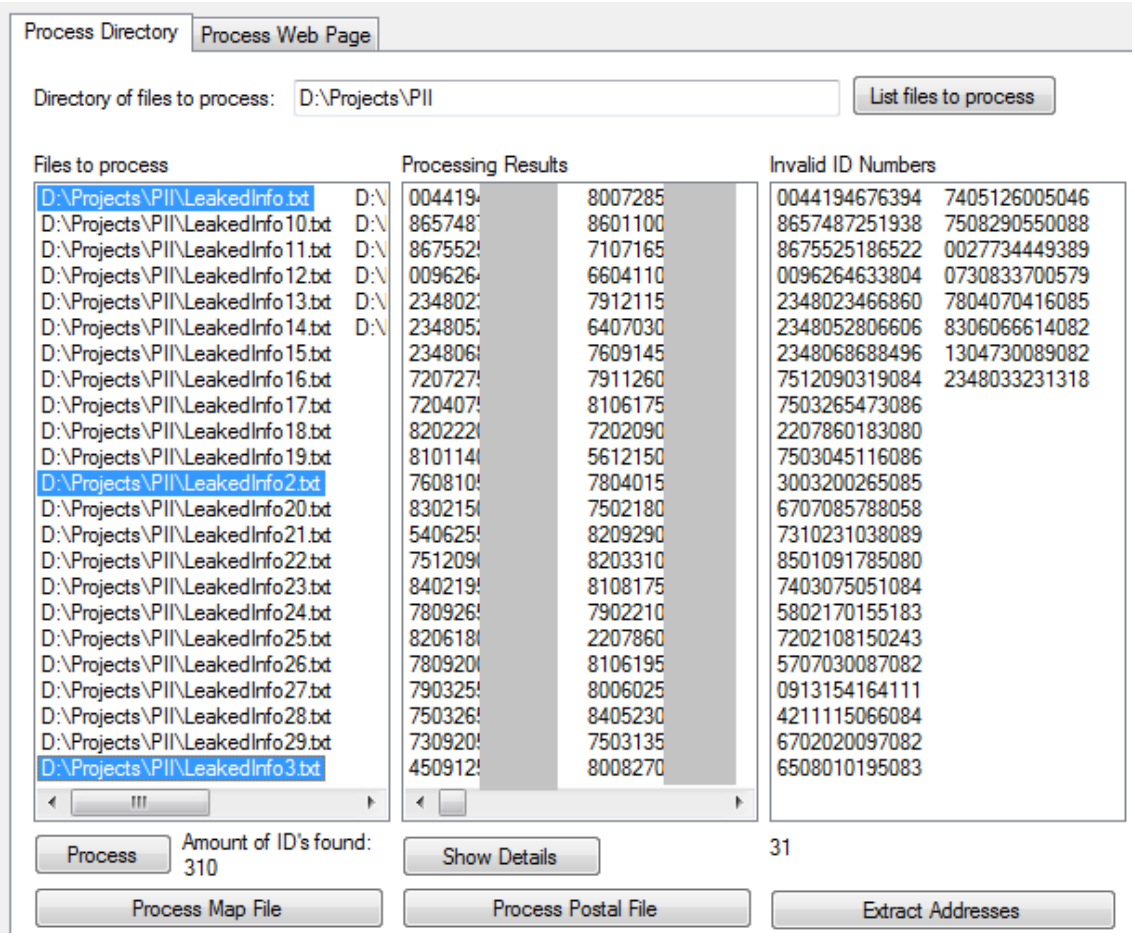

Figure 7-3: PII information extractor initial view

Once the initial detection of PII information is completed, the application automatically starts the verification process of detected information where possible. In the instance of ID numbers the structure should be as follows:

- ID number should always be 13 digits
- The first six numbers represent the birth date of the individual in the form YYMMDD
- Digit 7 represents gender with numbers 0-4 indicating female and 5-9 indicating male
- The following 3 digits indicate how many births occurred on the birth date for that gender
- Digit 11 indicates citizenship with 0 for South African and 1 for other
- Digit 12 was used in prior years to indicate the race of the individual
- Digit 13 is a checksum digit that makes use of a modulus 10 check to validate the consistency of the complete number

This type of validation serves the purpose of removing invalid data that might be included in the leaked dataset. In the example processing depicted in Figure 7-3, the need for this additional step becomes clear when examining the column marked "Invalid ID Numbers". While the system might at first detect numbers matching the general format of an ID number, it does not always match the explicit rules. No official government documentation regarding ID number validation could be located. Instead a number of private data sources were surveyed [87] and all provided correlating information.

Further information extracted from the data included physical addresses, email addresses, dates and credit card numbers as shown in Figure 7-4. PII detection and extraction limitations are discussed in Section 8.10.3.

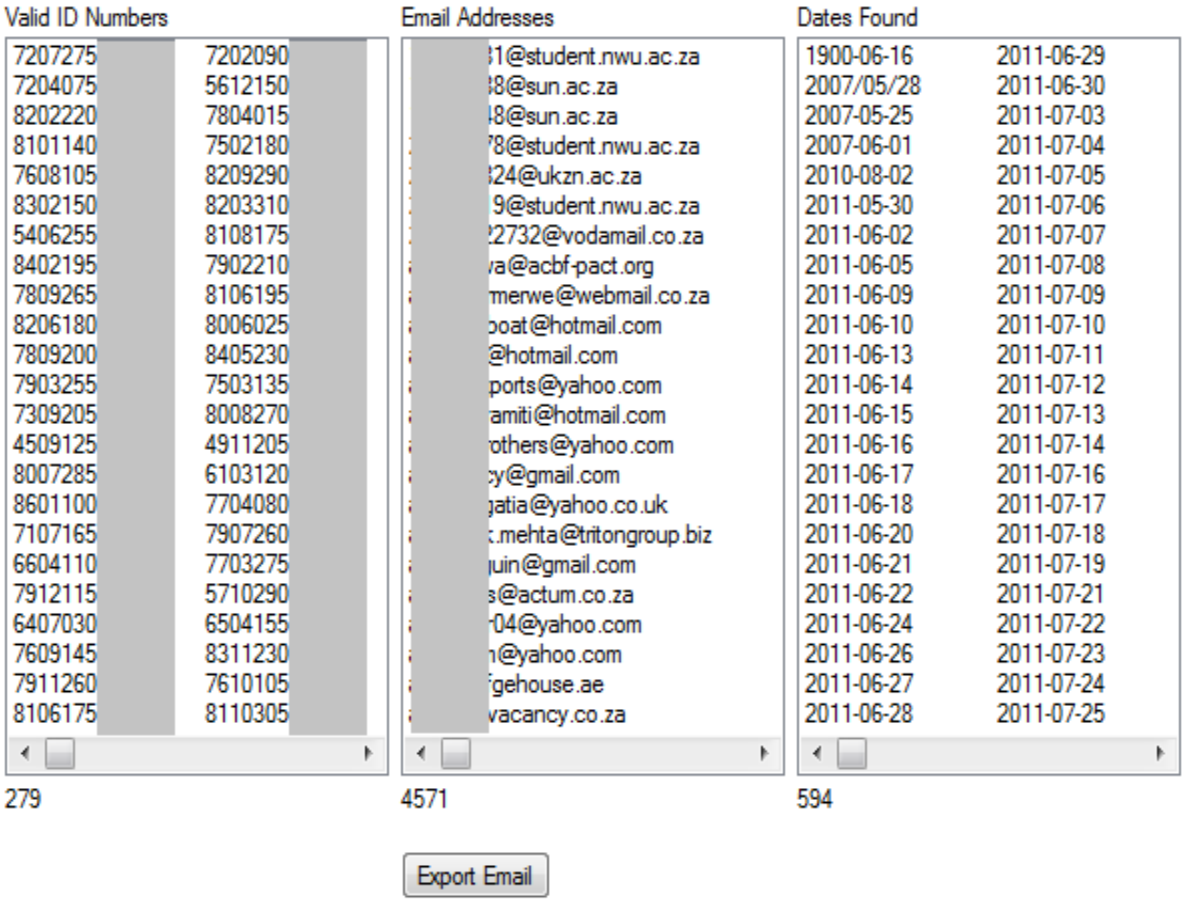

Figure 7-4: PII results view

[87] http://www.sadev.co.za/content/south-african-id-number-checker-excel-version-2

7.5 EXPERIMENTAL RESULTS AND ANALYSIS

While the system is only a prototype, some interesting discoveries have been made in the period that it has been operational for a temporal study. Several data sources from significant industry organizations have been flagged and a summary list of the most notable breaches is provided in Table 7-1. The dataset evaluated also contains manual data found in the six months prior to the completion of the system. These manually-detected datasets were used in the POC implementation of the system and made use of similar methodology for detection. In total the system examined 3964 records with 1970 unique IP addresses. The variance between examined records and unique IP address can be attributed mainly to the fact that one host can contain more than one file. Each file in turn has the potential to contain information that could be classified as having a breach or not.

Table 7-1: Notable incidents

Industry Type	Record Count	Type of data
Municipal	536588	Address, Surname, Account number
Technology	284995	Email, ID, Cell number
Health	4969	ID, Cell, Telephone
Insurance	172297	ID, Cell, Telephone, Address, Income

A summary breakdown of the varying types of PII was detected between 2013-12-12 and 2014-10-30 is available in Table 7-2. In total 2714 unique web domains were examined and PII was detected on 293 of these domains. This resulted in an detection ratio of 10.8%. While the number of unique domains detected from the selected data sources are nowhere near the 951700[88] claimed by the South African registrar, this is to be expected. Since no active scanning was performed in the system, detected URLs were limited to what was provided by the search engines used in the system. No real preference to the file extension PII was detected, since distribution was approximately even across detected URLs. PII was thus detected in all of the file types examined and no extension stood out above the rest.

[88] https://www.registry.net.za/domain_stats.php?gen=1&contentid=104

Table 7-2: Summary results of detected PII in South Africa

PII Type	Count
ID Number	892811
Land Line Number	852713
Cell Phone Number	1214516
Email Address	407307
Credit Card Number	78037
Address	537141
MD5 Hash	82
SHA1 Hash	13

The quantity of credit card and ID PII results highlighted a South African problem when attempting to discern this type of data in unstructured sources. The author discovered that in certain instances, a valid South African ID number can also pass the VISA character length and Luhn algorithm check. This complicates the classification of the detected number since the data type could be either an ID number or a credit card number. While it is common that credit cards have 16 digit numbers, it is not a requirement and can vary between institutions. A solution for this problem was to check each potential credit card number against the known banking codes.

A small subset of summary statistics for the data presented is listed below. While it seems improbable that an ID number from the year 1910 was listed in electronic records, manual verification revealed that the individual passed away at a advanced age and was therefore listed in an electronic obituary.

- Youngest person's detected birth date: 7th January 2000, Female.
- Oldest person's detected birth date: 9th January 1910, Male
- Number of times the same ID number was detected: 27
- Number of times the same cell phone number was detected: 4650
- Number of times the same credit card number was detected: 237
- Location most used for web site hosting: ZA for national, USA for international
- City most addresses were detected in: Durban

The hosting locations for servers that contained personally identifiable information also closely correlated with another independent study (van Rooyen, 2014). The study found that while the South Africa is the dominant hosting platform for servers hosting a .co.za domain, the USA was second on the list.

The instance of the cell phone number that was detected 4650 times also resulted in an in-depth investigation. The number was detected a large number of times since the company sales records were exposed. Each time the salesmen concluded a sale, an invoice was generated. The file containing a collection of these invoices was publicly available, and this was processed by the experimental system. From the data available in the file, it could have been possible to determine who the leading sales agent was. Since the company involved has a strong requirement for sales personnel, a rival could easily have gained an understanding of key personnel. Armed with the information, a slightly higher salary for the identified personnel to join a new company could have disastrous effects for the affected company.

Another interesting aspect that came out of the data is the number of instances employees make use of their work related e-mail for personal communication. The implication of this behavior is that in the event of a data breach at one company, the overall security posture of several others might be affected. Current breach notification legislation requires the company to notify the privacy regulator, who in turn decides if breach notifications should be sent to affected parties. These affected parties are typically the individuals directly affected by the data breach but not the companies whose employees were affected. Should an attacker attempt to target the affected employee, the company might also suffer losses.

The threat of phishing attacks breaching company security is a very real scenario, as previously explained in Section 7.2. By reviewing the results from the experimental system, it is possible to see which organizations' leaked PII data has the potential to affect other organizations the most. A breakdown of the domains affected is listed in Table 7-3.

Table 7-3: Top 9 South African domains recorded with breached emails

Domain	Number of times domain was detected
mweb.co.za	19433
statusib.co.za	18162
webmail.co.za	10605
getaways.co.za	6519
absamail.co.za	5766
vodamail.co.za	5174
sample.cybertrenz.co.za	4842
jdconsulting.co.za	4344
ultimatespray.co.za	3042

The data presented in Table 7-3 cannot simply be used to notify the potentially affected companies. The context in which these companies operate is also an important factor. Consider the highlighted data in Table 7-3 and bear in mind that the primary goal of those domains are to provide e-mail addresses to individuals. It is thus a realistic assumption that these entries into the list are due to the wide number of people using the domain for their personal email. Now consider the non-highlighted domains to realize that these are the domains that should be notified. Three scenarios that account for the presence of leaked information regarding an organization were detected during the examination of the experimental system results. The first scenario is that personal communication of the company was present in a data breach. This will account for the large number of clustered domain addresses due to employees' email addresses. The second scenario is that a large volume of employees subscribed to the same online service provider, such as a medical aid or pension fund. Should the service be hacked, the cluster of employee records will stand out. A third scenario found was due to a single e-mail address being detected a significant number of times in one file. Irrespective of the applicable scenario, the threat from data breaches has the potential to affect companies just as much as the employees.

7.5.1 GEOLOCATION OF DATA

The South African privacy legislation, the POPI Act of 2013, specifies that PII may not be placed in international locations without the consent of the data subject according to condition 6 Section 18(g) (South African Government Gazette, 2013). More explicitly, the data cannot be placed in countries with less stringent privacy legislation or it will be

considered a breach of legislation as defined by the yet to be appointed privacy regulator. By combining the hosting IP address with the Maxmind database, it is possible to geographically locate the data available on a given server. While a great deal of data is located in South Africa, there are plenty of breaches in international locations. By resolving the DNS entry of the website the PII was detected on an IP address can be obtained. By correlating it to a geolocation via the Maxmind database, a clear view of the current leaked PII distribution is available in Figure 7-5.

A single PII leak location is presented with a blue antenna icon. If a number of hosts with PII are located in closer proximity, they are grouped. This visualization effect is similar to the clustering found in the vulnerable host study presented previously in Section 5.13. Both data sources make use of the same visualization platform and fusion principles. The clustered group is then displayed in the form of a circle with the number of hosts containing any breached PII as described in Section 5.13.

A summary breakdown of the top ten hosting countries along with the number of hosts examined is listed in Table 7-4. The bulk of hosting is performed by South Africa and the United States, containing more than three quarters of all examined host data.

Table 7-4: Top 10 hosting counties of the PII experiment

Hosting Country	Number of hosts
South Africa	2022
United States	1289
Germany	225
United Kingdom	103
Russian Federation	38
Undeterminable location	31
Canada	28
Poland	25
China	23
Japan	22
Total	3806

Figure 7-5: Distribution of detected PII by host IP address

7.5.2 AVERAGE REMOVAL TIME OF DATA

The experimental system periodically rechecks the detected data sources. This was done in order to assess the normal removal rate of detected PII sources on the national domain. From the total 3316 potential leaks detected, the experiment results indicated that only 284 have been removed during the time the system was operational. The results indicate an approximate 8.6% self removal rate over the observed period for the available documents on the Internet.

Upon closer inspection, it was determined that the removal rate calculation of the data in the current experiment had a significant flaw. The experimental system only considered data removed if the file in which the PII was located in had been removed. This is not an accurate reflection of the real world and should be improved. Several instances were noted where the file remained in the same location where the initial breach was detected. In these instances the data in the file was altered and the breached PII had been removed. The original design specification of the system did not take this possibility into account, due the manner in which previous breach notifications occurred. In all previous instances, the complete file was removed and not amended to remove the PII it contained.

7.5.3 INTERESTING OBSERVATIONS

In one of the larger data breaches detected, the author felt compelled to contact the affected organization due to the sensitive nature of the data. The data breach was in the commercial insurance sector and contained records of all existing customers with current premiums, incomes, banking details and other related details. This type of data can severely damage a service sector company since competitors can simply offer lower costs for a period of time to entice customers to leave. Once the source of the data breach was identified, the responsible party was revealed. It was a smaller third party organization responsible for performing data analysis on the insurer's customer database to increase product offering and customer relations. Thus, while the insurer provided the data in encrypted format and ensured that both non-disclosure and minimum information security standards were specified, the third party organization had not adhered to these standards. This phenomenon has previously been documented in value chains where security is simply not the primary concern (Patnayakuni & Patnayakuni, 2014). While this was the most notable instance, manual examination found several other instances where data belonging to a company was detected on a third party's system.

7.6 SUMMARY

From the results obtained in this experiment, it can be proved that an automated system can indeed detect leakage of private information that has been on the web for an extended period of time. The type of data returned is also relevant to national cyber security and as such, the results of the experimental PII detector was incorporated into the fusion system. This in turn allowed for successful visualization in the same framework as the host vulnerability data. The system serves to prove that automation will increase the detection rate to reduce the average time that data is unguarded. An automated system has the added benefit of reducing the chance that the discovering party makes a copy of the leaked data, thereby compounding the original loss problem. Various technical issues remain in the construction of an automated PII detection system and are not trivial to resolve. However, the potential has been demonstrated for an automated discovery system that could be extended to provide a national detection ability for the appointed privacy regulator. Funding for the implementation of such a system is always a contentious topic but research performed has shown selective taxation might be a viable option, considering the potential gain to the national economy and individuals alike (Piquero, Cohen & Piquero, 2011). In conclusion, PII intrigues everyone, educated and uneducated alike, and has to be protected lest it be used against the very systems designed to make use of it.

This chapter is the final chapter in PART II of this document and examined the results of the custom created PII sensor. The purpose of the PII sensor was to provide information regarding the human component of the national attack surface. The information obtained, in conjunction with the information made available by the sensors used in Chapter 6 serves to provide information regarding all three components of the attack surface discussed in PART I, Section 3.2. While the information obtained by the PII sensor is stored in the same system, adheres to the same fusion rules and is visualized in a similar manner as the infrastructure sensor data, the information has not been fused to its maximum potential. The PII information obtained regarding the human component are typically stored on infrastructure similar to those discussed in Chapter 6 and the storing of personal information should thus be made an attribute of the appropriately identified infrastructure object. The first chapter in PART III, Chapter 8, examines the potential that exist to increase the fusion between the different sensors. The chapter further examines the experimental system results obtained against the five JDL model levels.

PART III

Analysis, evaluation and conclusion

Be careful and you will save many men from the sin of robbing you.

Edgar Watson Howe – Newspaper and magazine editor

8

Research analysis

8.1 Introduction

Previous chapters discussed the system architecture and individual detection methods. Chapter 5 presented the fusion model and programmatic architecture of the application. Chapter 6 presented a case study that focused on the detection of infrastructure making use of the Shodan dataset and various vulnerability databases. In Chapter 7, the focal point was moved to the human component of the attack surface, in order to examine PII detection by means of another case study.

Building on the knowledge previously presented, this chapter will review and extend the work performed in the previous chapters to highlight the current fusion system's achievements and limitations. The limitations of each of the individual detection methods will also be assessed with possible solutions where appropriate.

8.2 Validation of adapted JDL model

The adapted JDL model presented in Chapter 5 described the proposed steps and order required for cyber data fusion on a national level. The aim of the model was to provide a structure for processing data sources that has the potential to increase national cyber situational awareness. Currently available data sources that have the potential to provide information at a national level were discussed in Chapter 4.

Full validation of the model is unlikely to occur without an extensive period of testing and a significant amount of resources. With this in mind, partial validation of the model was performed with the results of the experimental system. The experimental system made use of selected data sources, fused them in the manner described by the adapted JDL model created in Section 5.4 and evaluated the results obtained. Results were discussed in two main case studies detailing aspects of the investigation. Validation of the model will be discussed per JDL level in the following sections.

8.3 JDL LEVEL 0

This level is primarily concerned with the cyber sensor data extraction and data alignment, as discussed in Section 5.8. In the experimental system, extraction of data was successfully achieved by obtaining data from various cyber sensors such as:

- Shodan
- CVE libraries
- Custom Leet speak libraries
- Custom PII Detector
    - Google
    - Yahoo
    - Bing
    - Twitter
- Maxmind

The sensors selected by the experimental system are a subset of the currently available resources; reasons for specific selection was presented in Section 5.6. Chapter 4 contains more examples of potential sensors that could be incorporated in future experiments. The extracted data were examined for entity properties such as IP addresses, hostnames, open ports and other identifying characteristics.

To facilitate the number of cyber sensors used, as well as the volume of the data presented by these sensors, an iterative approach to importing the data was taken. Data regarding the various datasets were not imported into a single table, but each dataset contained a normalized table structure depending on the data provided. Once this was completed, extended data alignment was performed on the datasets to identify first order entities as well as corresponding properties. The benefit of this approach became evident after experimentation revealed that it is not always possible to fuse the obtained data sets together in any reliable way. The correct identification of first order entities are described in the following section.

8.3.1 EXTENDED ALIGNMENT OF SENSOR DATA

The case studies presented in Chapters 6 and 7 each focused on specific types of information relating to different aspects of the national attack surface. Chapter 6 focused on finding information regarding the devices located in the South African Internet domain as defined in Section 2.7. Additional data sources were then used to enrich the dataset of devices to identify potentially vulnerable devices. This was done with the aim of showing the vulnerabilities available in the hardware and software

component of the attack surface as described in Section 3.2. Chapter 7 focused on finding personal information regarding individuals on the Internet to assess information related to the people component of the attack surface description. In the following section, the potential for extended fusion of the identified entities in Chapter 6 and Chapter 7 will be discussed.

8.3.1.1 FUSION BY IP ADDRESS BETWEEN DATASETS

Although the focus of the datasets used in this study are different, all of the data sources contained information related to the defined South African Internet domain. This presented the experimental system with the opportunity to fuse the datasets together to obtain additional information previously not available. For example, by fusing a host detected by Shodan to a host that contained leaked PII information, the entity that was created at Level 0 of the JDL model is enhanced with additional identifying properties. For the Shodan dataset of 2013-09-10 (containing 693481 unique hosts) and the currently detected PII database of 2014-10-28 (containing 3964 unique entries), the following results were obtained. When the data is fused on IP address: a total of 917 hosts were identified that matched both datasets.

Assessing the detected hosts for vulnerabilities resulted in the identification of 134258 detected potential vulnerabilities with an average CVSS of 7.8. With an infrastructure dataset containing information regarding 693481 devices in the South African IP range, 917 hosts that leak PII constitutes 0.13% of all devices. These results are enticing at first glance since it seems to establish proof that hosts with a higher than average CVSS score have a greater chance to leak PII. From the case study presented in Section 6.3, the average CVSS score detected was 5.24 as opposed to the hosts that leaked PII with a average of 7.8.

8.3.1.2 LIMITATION OF FUSION BY IP ADDRESS

A key problem with the results highlighted in Section 8.3.1.1 is that the temporal differences between the two datasets are ignored. The temporal discrepancy exists due to a number of factors including the constant assignment and renewal of IP addresses by DHCP servers. Another factor is the manner in which ISPs host content. The online content hosted by the ISP can be distributed to various servers without interrupting availability. A DNS update is all that is required for the resolution of the DNS name to be redirected to a new location. Thus a new IP will be obtained for the content location on the Internet but service would not have been interrupted for anyone wishing to access the hosted content.

As an example, consider a website from the PII detection sensor data. The website www.skysun.co.za contains no detected PII, and resolved to 181.224.135.17. Further investigation from the Maxmind online service indicated that the server used to host the website content was as of 2014-10-23 located in the United States, Chicago. Now consider that at the time that the PII sensor detected a potential PII leak on the server, the IP address was 108.162.196.197 and that the website was hosted in the United States, San Francisco. The example discussed here will, at most cause a discrepancy at town level regarding host location or vulnerabilities detected. In other instances, the variation could be much bigger resulting in incorrect placement by even continents. Without the historic information of where a domain resolved to at a specific time, the accuracy obtainable from the fusion process becomes unreliable.

A key requirement to facilitate the higher-level fusion of different datasets based on IP address thus requires comprehensive DNS history records. These records can facilitate the mapping between DNS name and IP address over time. While every effort was made to obtain a DNS history repository to extend the experiment, no currently maintained source has been uncovered in this research. A project named the DNS History[89] service is available, but has not been maintained since late 2013. Even if the DNS source was maintained, a search in the available records did not uncover any .co.za DNS update records.

8.3.2 ALTERNATIVE APPROACHES

IP addresses, as discussed in Section 8.3.1.2, are not always a reliable device identifier on the Internet. DNS record retention can limit the inaccuracies that arise when matching on device IP address, but cannot eliminate the problem altogether: in the event that a company / individual manually re-assigns statically allocated IP addresses between devices with no DNS, the previous approach will fail. This is one possible scenario where DNS record retention will not suffice to account for all device movement, more scenarios exists.

Therefore, a unique device identifier is required to accurately identify a device across different datasets regardless of IP address. Server hostnames are considered better identifiers than IP addresses but this property is also not static and can change over time. Previous work has indicated that devices on a network can be uniquely identified by clock skew (Kohno, Broido & Claffy, 2005). Clock skew refers to the millisecond

[89] https://dnshistory.org/

variance introduced by each device's internal clock when a timestamp is generated for network traffic communication. Further work on this approach has confirmed the possibility of identification and even extended the work to show the potential for counting devices behind NAT (Polcák, Jirásek & Matousek, 2013). However this type of approach requires the ability to receive a number of Transmission Control Protocol (TCP) packets in transit from device to requested location. Since the national Internet is typically not controlled by Government, the method will only detect a portion of the potential devices barring contribution from ISPs.

8.3.3 LEVEL 0 SUMMARY

The Level 0 validation of the model proves that it is possible to combine information from a variety of data sources to present a representation of entities in the demarked national cyber domain. Care should however be taken to recognize the fact that these cyber sensors do not necessarily report on the same IP address in the same temporal span. As such, it might be preferable to identify entities from various cyber sensors, without attempting to align their data. This will result in the identification of more hosts than what really exists, but will still allow higher order layers of the JDL model to infer future state.

8.4 JDL LEVEL 1

In the previous level of the JDL model, objects were created and an attempt made at aligning all available data to ensure that objects identified are not duplicated. As discussed in Section 5.9, the purpose of Level 1 of the adapted JDL model in the cyber domain is to enrich the objects identified with all available data pertaining to the object. To achieve this, the case studies presented in Chapter 6 and Chapter 7 made use of public data sources to enrich the data detected from the primary data source. Metadata sources (such as NIST CVE libraries) and geolocation data sources (such, as those available from Maxmind), added additional properties to the objects created at Level 0.

Enriching the detected hosts in this fashion immediately adds increased value to the dataset and provides information not previously available. The metadata sourced from Maxmind that contains geolocation data regarding devices in a region was added to the host objects identified at Level 0. This allowed analysts to make use of the system to bind an IP address to a region. The benefits of host geolocation were examined and presented in Sections 5.9 and 6.3. It should be noted that Section 6.3 presents the data in a visual format that is not strictly correct for Level 1 representation. The data at

Level 1 is typically at a raw level and often represented in text or in database format. The images representing the data obtained from Level 1 are only created at JDL Level 5 and merely serves as illustration.

Similar to the work performed by Giacobe (2012), the addition of vulnerability data to the host objects defined at Level 0 served to further enrich the available properties of the objects. Information regarding the hosts, services provided or location of the host was fused with information regarding attacks the host might be vulnerable to. CVE has previously been described in Section 4.5.7 as a very inaccurate measurement of true vulnerability. Unfortunately, it is also at present one of the only options available for vulnerability indication. By adding CVE databases between 2004 and 2014, the number of vulnerabilities obtained was 12123064, as discussed in Section 6.3. This number is extremely large but does not address all known vulnerabilities for the South African domain. As discussed in Section 4.5.9 and Section 6.7 incorrectly configured devices are often a critical vulnerability to organizations. In the instance described in Section 4.5.9, the open resolver project maintains a list of incorrectly configured DNS servers. Importing the results from this database will add additional properties to the objects created at Level 0, allowing visualization, reporting and potentially resolution. However, there is no comprehensive data source for vulnerable routers as described in Section 6.7. To add these vulnerabilities to the dataset, analysts that make use of the experimental system will require an interface to the working dataset. While applicable to Level 1 properties, this action presently requires a skilled professional. As such, while the information may be added to a Level 1 object's properties, the actual functionality is only provided at Levels 4 and 5 of the adapted JDL model.

Critical infrastructure is mentioned in nearly all the national cyber security policies discussed in Section 2.8. Unless a source of critical infrastructure is already available, Level 1 is the appropriate place to perform classification of this kind. Previous research has indicated that it is possible to differentiate normal ICT devices such as routers and laptops from SCADA devices such as PLC controllers (Caselli et al., 2013). It should be noted that normal ICT devices can also have a critical infrastructure role and the presence of a SCADA equipment does not immediately indicate critical infrastructure. The use of the JDL model to process information regarding critical infrastructure has also been demonstrated by Timonen et al. (2014), while the use of Shodan data has been proven to provide assistance with critical infrastructure detection (Williams, 2014). Detecting the actual infrastructure is

not simply a matter of performing a few queries on the available datasets. Searching for key terminology such as power, water, electricity, critical or supply, results in a long list of inaccurate results. Previous research indicates that the focus of the search should be based on keywords that identify devices typically used in critical infrastructure applications (Radvanosky, 2014). This is similar to the work performed in Section 6.7 that located potentially defective routers by searching for identifying keywords.

A limitation of the current system is that no international assets could have been identified by the current system. Critical infrastructure is often not located only nationally but internationally (Clemente, 2013). Since datasets used in this experiment focused on the South African domain, no international assets would have been detected. Another limitation is that even with identification of critical infrastructure, the dependencies between devices are often the most critical (Rinaldi, Peerenboom & Kelly, 2001). To discover the links between devices would be hard to achieve with current datasets.

8.4.1 LEVEL 1 SUMMARY

The successful addition of extended properties to the objects created in Level 0 was demonstrated at Level 1. Examples of how a host located in the cyber domain can be classified as vulnerable or not have been demonstrated. This validated the adapted model up to layer one for the purposes of this research. The information obtained at this level, relevant to the physical domain, has the potential to provide national cyber security policy makers a view into the types of devices located in their borders. In addition, the number and types of vulnerabilities identified are potentially valuable to a range of different audiences. For policy makers, it will provide a view into the number and severity of vulnerabilities available.

Priorities could be set based on different host classifications, or the types of vulnerabilities present. Should it be possible for commercial entities such as SMEs to make use of the database, it has the potential to provide them with information regarding their infrastructure. While this will not solve the technical problem experienced, owners will at least now have an indication of the risk that they are exposed to in everyday operations. While this type of interaction with various entities might only occur at Level 5 of the model, Level 1 is where the information to be presented is created.

8.5 JDL LEVEL 2

As discussed in Section 5.10, Level 2 of the JDL model moves the focus away from individual objects properties towards the aggregation of related object properties. The

aggregate functions used should focus on identifying and mapping the relationship between entities and events.

In the experimental system constructed, the function of this level was achieved in a variety of ways. The ability to group devices according to a predefined geographic location was illustrated in Figure 6-1, Figure 6-2 and Figure 7-5. This is not the only type of grouping available and the clustering of devices per vulnerability severity has also been illustrated in Figure 6-5. Even though the datasets are different, the grouping capability for both the infrastructure devices visualization as well as the PII leakage hosts remained constant.

The main drawback of the current system at this level is that the data sources used in the experiment does not provide information regarding specific events. This limits the inference of actions between the objects defined at Level 0. In order to achieve the full potential of this level, a data source that records events between hosts should be incorporated. While the introduction of such a data source will suffer similar limitations on a temporal level for data fusion as discussed in Section 8.3.1.1, future work may address this limitation.

8.5.1 LEVEL 2 SUMMARY

The aggregate functions provided by Level 2 have the potential to be extremely valuable for national cyber security policy implementation. Achieving inventory of devices available on the national network has previously been identified as a key requirement for successful policy implementation in Section 2.10. Consequently, the objects created at Level 0 and enriched at Level 1, which already contain all the information required, can be grouped and analyzed in a variety of manners. While the information at Level 2 is still in a very raw format not specifically tailored for human readability, it is the input data for clustering visualization techniques such as heat maps and choropleth techniques. As such, the information obtained at this level will be used at Level 5 for effective visualization.

8.6 JDL LEVEL 3

Level 3 of the adapted JDL model is the culmination of processing all information available in order to present a future state of the system under observation. As such, it is also the hardest to accomplish. Level 3 as discussed in Section 5.11, has a strong similarity with Level 2 in terms of aggregation and grouping but has to consider the present state and also potential future states. In the current experiment, the lack of

event data made it difficult to implement functionality at this level. Limited examples of Level 3 activity exist and will be discussed.

The experimental system does not perform any scanning to ensure compliance with legal requirements, as explained in Section 2.9.3. Therefore the only temporal data processed by the system is made available when datasets are periodically refreshed. For the infrastructure data, the Shodan dataset is required as listed in Table 6-1. Similarly, information regarding the breaches that involve PII is placed on a temporal timeline as presented in Figure 7-2. From the results of these datasets, the system could add the functionality to calculate average growth rate and projected future population of devices present. Similarly, the average number of leaked records on a yearly basis could be estimated with enough prior information in the system.

8.6.1 LEVEL 3 SUMMARY

Implementation at this level is currently problematic with limited open source datasets available. Level 3 of the JDL model has a significant temporal characteristic and the datasets available for current evaluation are decidedly static in nature. Further implementation of this level will either require a real time integration with third party data sources, such as the real time attack feeds discussed in Section 4.5.6, or the implementation of real time scanning. The successful implementation of this level has significant potential for national cyber security since the potential to predict future infection exists. Aggregate measurements indicating the number of devices affected by a specific vulnerability have the potential to provide quantifiable information regarding the losses that could be suffered. This type of information in turn, could assist CERT personnel to determine the highest priority task during an outbreak.

8.7 JDL LEVEL 4

Previously discussed in Section 5.12, the function of Level 4 is that of process refinement. As such, it is not strictly considered a fusion level but a management level in the JDL model. In the current experiment, the most visible implementation of this level is available in two functions. To refresh the datasets available to the system, the data made available from either Shodan, Maxmind, NIST or the open source APIs has to be imported for processing. The functionality mandated by Level 4 selects what data source dataset to import and is responsible for ensuring that imported datasets are uniquely numbered. Log keeping of the process is also recommended should the need for future auditing occur. A screenshot of the functionality is presented in Figure 8-1 to

illustrate how the management level can keep track of what action was performed regarding each sensor.

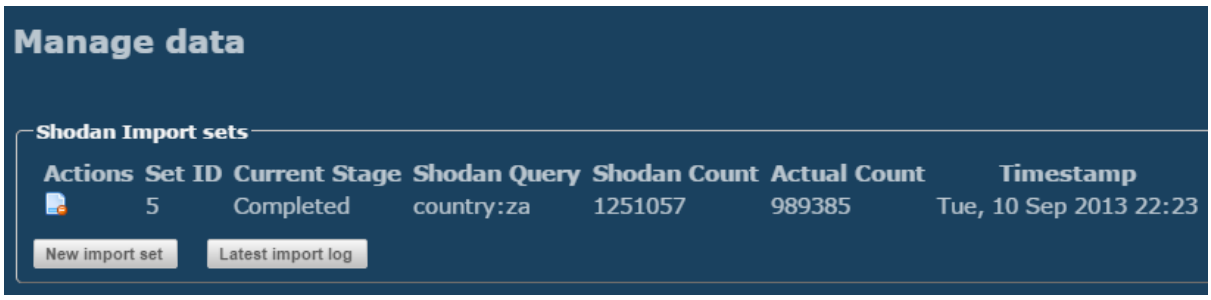

Figure 8-1: Shodan data import functionality

The potential functionality of Level 4 can be examined by considering the work presented in Section 6.7 regarding vulnerable routers. Most vulnerabilities in the current system were obtained from documented CVE libraries. However, these sources do not provide information regarding all possible vulnerabilities and the potential to describe custom vulnerabilities therefore exist. The devices described in Section 6.7 could have a severe impact on organization operation or even national operation, but are not typically listed in CVE advisories. At least in the instance of incorrectly configured DNS servers, as discussed in Section 4.5.9, the information is available from the Open Resolver project. Should it become possible to obtain the data from the curators, it could be imported into the current dataset in a similar manner to other datasets. There is currently no known source of information tracking these types of vulnerabilities discussed in Section 6.7. As such, should a analyst become aware of a vulnerability that needs to be incorporated into the current dataset, access to the underlying data will be required. To achieve this functionality, the ability to create custom host classification rules are necessary. An example of this functionality in the experimental system is available in Figure 8-2.

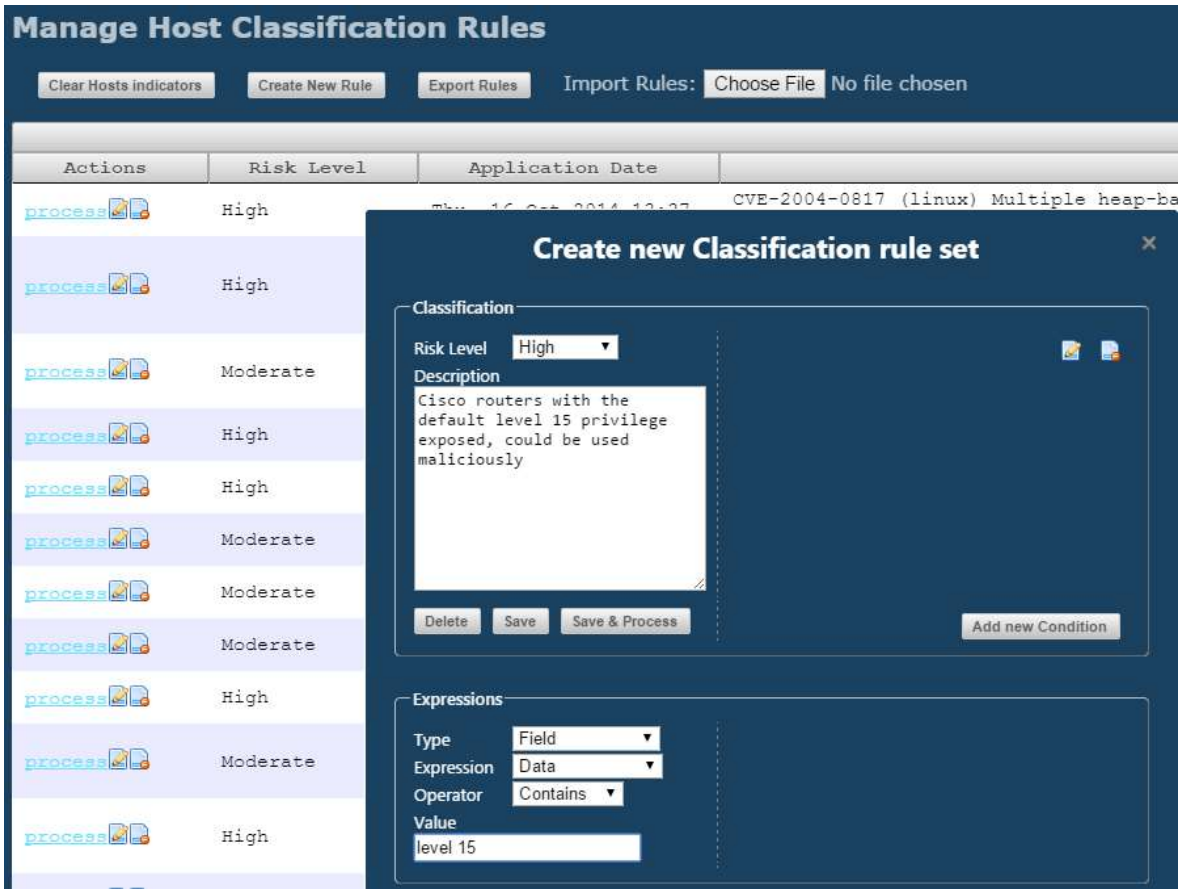

Figure 8-2: Custom host classification rule creation

8.7.1 LEVEL 4 SUMMARY

The potential to alter the current fusion process is required as more experience in the process is obtained from both the operators and the developers of the system. Should policy implementers discover new datasets available, a generic process for the system should already have been identified. These processes to import and refine data, are all functions of Level 4 of the JDL model and has been demonstrated in this section.

8.8 JDL LEVEL 5

Several Techniques were utilized to effectively implement visualization in Level 5. One of the most used techniques was clustering of related entities. Clustering is an effective method of visualization since it visually conveys the relationship between entities without the need to explicitly state what the relationship is (Meier & Heidmann, 2014). Several variations of clustering have been documented and in this experiment the following variations were utilized:

- Heat maps – One of the most widely used visualization techniques in use today with a wide range of applications in a variety of disciplines (Wilkinson & Friendly, 2009). A heat map is a representation of quantifiable values applied

over a defined region that could typically be used to display intensity or distribution of entities. Previous use of heat maps in information security on a national level was performed when the outbreak of the Conficker worm was examined (Irwin, 2011).

- Marker clusters – A grouping of markers in close proximity to each other (Delort, 2010). Several implementations of this type of grouping has been found in geolocation applications such as Google Maps and Bing maps.
- Choropleth – This relies mainly on the variation of shading between predefined objects and is typically used in geolocation applications for thematic information visualization (Andrienko & Andrienko, 1999). In the experimental system, choropleths were used to indicate the different regions within South African borders.

Clustering, if implemented with a specific purpose, has the benefit that it reduces the volume of information that the operator of a system has to deal with. This is achieved by first providing an overview of all related objects, allowing the operator to zoom to greater details and then to provide detailed information. This type of details approach has a long history in visualization theory and was proposed as a set of seven tasks (Shneiderman, 1996). Additional proposed tasks include the ability to filter, keep a history of user actions and to allow the user to further refine a filter through an extract step.

8.8.1 LEVEL 5 SUMMARY

Effective implementation of Level 5 was demonstrated. The visualization component has the potential to add value at a national level by presenting the raw data obtained from prior levels to policy makers and implementers effectively. Limitations of the visualization component should be addressed in future iterations of the system to ensure that it sufficiently provides the information required by different role players in the national cyber domain.

8.9 ADAPTED JDL MODEL SUMMARY

The choice of the JDL model provided a standardized method of implementing the various layers of information fusion applicable to national cyber security policies. In this experiment, only static data sources such as Shodan and CVE vulnerabilities were demonstrated, but real time integration of data is definitely possible. Through the use of several embedded case studies, the adapted model proposed for use in the national cyber

domain functionality has been substantiated. In the following section, practical experiment limitations experienced will be discussed. The information provided in the following sections is separated from the discussion of the JDL model, since it is related to, but not directly applicable to the JDL model validation.

8.10 Practical experiment limitations observed

While the potential to effectively detect and visualize various information security aspects affecting a nation has been demonstrated, a number of limitations were identified. The limitations affected not only the individual cyber sensors providing the information but the overall fusion system as well. The limitations detected will be addressed first on a complete system level and then individually on a sensor level. The infrastructure detection limitations will be discussed in Section 8.10.2 and the PII detection sensor limitations in Section 8.10.3.

8.10.1 System level limitations

Limitations identified on this level affected the global operation of the experimental system. The limitations identified in this section, affects all sensors, unless a specific data source negates the identified limitation by providing countering information.

8.10.1.1 Third party reliance

Since the system makes use of commercial or open source datasets, it is reliant on the external vendors for updates to the required infrastructure. While this is the point of the current experiment, it is also a limitation worth mentioning. In the three year period of this experiment, three documented data sources have been discontinued. While it is often possible to switch to an alternative data provider, the data provided may require rework of existing infrastructure. In the instance of the discontinued DNS history service, no other suitable replacement could be found. This is crucial for the data fusion process to establish a temporal link between entities. In the implementation of the PII detector, only data breaches that have been indexed by a service provider can be detected.

8.10.1.2 Resolution of detected vulnerabilities

Contacting persons responsible for a vulnerable system remains a manual task that is currently hard to automate. Typically the contact information for the person responsible for the vulnerable device/software on the Internet can be obtained to a limited degree via a WHOIS query. Unfortunately this is not always possible if the device that has a

vulnerability is a router with a dynamic IP address. Should a system such as this be implemented, the co-operation of various ISPs would be required to effectively inform end-users. In addition to actually finding the vulnerability, some form of government agency, national department or appointed contractor would have to be available to assist the contacted personnel to correct the detected vulnerability should they not have the required skill themselves. This has been effectively implemented in the USA where the National Security Agency (NSA) will assist a company to secure their internal networks according to the national security specification. Various types of information security sharing standards are available as listed in Table 8-1, but no single application surveyed makes effective use of this.

Table 8-1: Information security sharing standards (Beaudoin et al., 2010)

Standards	Vulnerability	Threat	Safeguard	Test	Incident	Action	Asset	Operations	Risk
CVE	X	X	X	X	X		X		
NVD	X								X
CVSS	X	X							
CPE	X	X	X	X	X		X		
CCE			X	X		X			
CAPEC		X			X				
CWE	X	X			X		X		
MAEC		X			X				
CME		X			X				
NVG		X			X	X	X	X	X
KML		X			X	X	X	X	X
CRE			X	X	X	X			
ERD			X	X	X	X			
OVAL		X	X	X					
XCCDF		X	X	X					
CRF				X			X		
IODEF					X				
VerIS					X				
CEE					X				
IDMEF					X				
NASL			X	X					
Snort Rules			X	X					
Regex			X	X					
ISO-27005									X
ISO-8601	X	X	X	X	X	X	X	X	X

The experimental system examined in this research primarily makes use of CVE data to detect vulnerabilities. The potential exist to obtain a more detailed operational picture by incorporating more of the available standards from more sources.

8.10.1.3 VISUALIZATION LIMITATIONS

During the construction of the experiment, several case studies were performed regarding either the infrastructure of a company or the leaked PII component. In most instances, the visualization system was more than sufficient and provided ample feedback to the operator. One important exception arose when a representative of a company that provides internet backbone infrastructure to research institutions asked if their ASN range could be examined. This relatively simple request immediately highlighted a serious oversight in the design of the current visualization component. While possible to search by IP address such as x.x.x.x and even IP range such as x.x.x.x/24, searching for numerous IP ranges allocated to a company is not possible all at once. Considering that the company in question had 66 different ranges allocated to them, this presented a serious challenge. The solution is not complicated, but will require improvements to the current system. It is expected other such issues will be encountered with future operational use.

Another limitation identified is the manner in which the current system processes information in the browser window of the client. At the start of the experiment, the datasets were sufficiently small enough to load all components in the browser for processing. The visualization system was tested to handle up to 50 000 different objects with ease but the datasets used exceeded growth expectations. With the latest Shodan dataset purchase, 693481 unique objects were identified, well over the 50 000 the system could comfortably handle. Although the PII host data is significantly smaller, the dataset was not insignificant and added more than 3000 available hosts. With this in mind, combined with the temporal limitation identified in Section 8.3.1, the need arose to separate the information obtained into both manageable and useful information. Both datasets were thus available in the same system but the visualization of the datasets were implemented on different levels. This provides the ability to effectively make use of both datasets in the same visualization system while focusing the view presented to one type of vulnerability.

8.10.2 Detection of Internet facing infrastructure limitations

This section will critically examine the limitation of the system that was used to obtain information regarding the devices located on national infrastructure. While the data was predominantly obtained from Shodan it was enriched with CVE data as explained in Section 5.9 on Level 2 of the adapted JDL model. In future, several other data sources could also be added to the system. The limitations identified are not due to a lack of data sources. The limitations would still be relevant unless the data source itself provided enough information to negate the limitation identified.

8.10.2.1 Inability to accurately detect vulnerabilities

The current implementation of the system will almost certainly suffer from a lack of vulnerability detection accuracy. While CVE libraries are useful for determining the potential vulnerabilities available to a platform, they are by no means a guarantee that the vulnerability exists on a system. To obtain certainty, a manual inspection is almost always a requirement as discussed in Section 2.10. A data source such as the Open Resolver project discussed in Section 4.5.9 is an example of a data source that can negate this type of limitation to a partial degree. While the data from the Open Resolver project would identify a incorrectly configured DNS server vulnerability as a certainty, the data would still not contain information regarding normal CVE vulnerabilities.

8.10.2.2 Inability to protect devices

Bass (2000) describes the Gamma problem where the network placed under monitoring should be slower than the monitoring network or the attack could have succeeded without prior warning. With the present system this remains true. The information obtained is informative and can be used for trend analysis but is not real time and will thus not show a attack as it happens.

8.10.2.3 Processing limitations

As the number of devices detected grows, so will the processing and storage requirements of the system. Importing the obtained Shodan data proved too slow with a normal console application since the data was all text and therefore expensive to parse, compare and process. Since the identification of potential vulnerabilities was performed during the import process, this required the processing of yet another big file. To address this, an increase in processing speeds was obtained by creating a multi-threaded importer. While currently effective, it is not a permanent solution. As more and more information becomes available from a data source such as Shodan, the process

gets considerably slower. Importing a 314MB text file while applying CSV processing is surprisingly slow on even a relatively powerful computer. It is recommended that the importing of data be separated from the processing of the data since processing in databases typically results in performance gains over files.

8.10.3 PII DETECTION LIMITATIONS

The PII detection sensor was created to partially monitor the human aspect of the national attack surface as identified in Section 3.2.3. The system had considerable success in the identification of data breaches (as discussed in Chapter 7), by making use of open source systems. Despite the success, several limitations have been identified in the current experimental implementation. The limitations identified is in addition to those identified in Section 8.10.1.

8.10.3.1 AUTOMATED PROCESSING OF UNSTRUCTURED DATA

Automatic processing of unstructured data is currently very inefficient and extremely hard to achieve. Humans have an almost automatic ability to grasp the layout of a file that is hard to replicate in current machine processing techniques. A human can tell if the field/word/number next to a previous field/word/number is related and should be processed in conjunction. Achieving this type of context with automatic processing requires substantial metadata, a known file layout or previous knowledge on how to proceed. The current system has a rudimentary method of evaluating the file under investigation layout, but substantial improvement is required to decrease false positives.

8.10.3.2 INCREASED PERSONAL IDENTIFICATION DATA TYPE DETECTION

The currently implemented detection of leaked passwords relies on the ability to detect hash sequences from a variety of hashing algorithms, typically used for password storage. Passwords are not always stored in hashed format despite it being a fundamental security recommendation. In the absence of hashes, the current detection methods fails to detect the leaked PII. As a potential solution, keyword comparisons and evaluation against common passwords would allow the system to retain the ability to detect leaked passwords.

8.10.3.3 HUMAN LINGUISTIC TENDENCIES

Spelling is currently a limitation in recognizing personal information that is non-numerical and typically captured by a human. Since humans make typographical and spelling errors the data is not trivial to detect. Even if the spelling is correct, the variety of common acronyms require significant additional processing. Addresses are one

example of this type of data and might serve to explain the low detection number in this PII data type. The research application of natural language processing and fuzzy machine learning techniques could improve matching of disclosed data types such as addresses.

8.10.3.4 VARIETY OF LANGUAGES

Language is an often overlooked barrier that exists in many computing applications. While numeric PII will still be detected with relative ease barring any formatting and layout challenges, other types of PII will definitely be missed if alternative language detection is not made available. Even numerical values will fail as soon as numeric representation is altered to a different standard from the current western standard. Given that South Africa has 11 official languages, this is a very real consideration to take into account.

8.10.3.5 REGIONAL REPRESENTATION

Regional representation of PII is important since ID numbers, telephone numbers, addresses and a variety of other PII are stored differently depending on geographic location. South Africa is fairly uniform in the manner of PII representation but difficulties are present. Consider the possible entropy in a small category of data such as valid number plate standards. In South Africa a number plate is typically eight characters long but custom number plates are valid when registered. Identifying the information from a photo or car is completely possible with current technology. As soon as the eight digits are detected in an unstructured file however, there is no real method of ensuring that the numbers belong to a number plate, it is just a random eight characters. Most national identification numbering schemas have a form of parity check that can be calculated, but this is not foolproof as described in Section 7.5.3.

8.10.3.6 FILE AND OPERATING SYSTEM DIFFERENCES

Encoding of characters, whitespace and line endings can make analysis of a file unreliable (Aura, Kuhn & Roe, 2006). Different operating systems represent line endings and character encodings differently. If a character representation is not recognized, valid PII information can go undetected due to the encoding differences.

8.10.3.7 FALSE DETECTION

The ability to distinguish between leaked and published business information is a significant requirement. Not all PII found on the Internet is leaked. There are a variety of valid reasons for available PII and therefore an effective system needs a mechanism

to distinguish between valid and leaked PII data. A relatively simple machine learning technique could be implemented to reduce the amount of false positives in the detection sample. Alternatively a threshold could be specified to determine when the information detected classifies as a data breach.

8.10.3.8 LIMITED DATA SOURCES

The ability to perform real-time detection of PII on South African networks would have great potential to increase the efficiency of such a system. Work has previously been conducted in the detection of PII and PHI, specifically in P2P networks (Sokolova et al., 2012). The inclusion of these types of data sources will increase the detection coverage of the system.

8.10.3.9 INCREASED INDEXING AND REPORTING

As part of the system operation, the current system routinely re-examined previously detected PII sources. This was done in order to track instances where the data has been removed. The selected approach was to verify that the file containing the leaked PII is still available at the detected URL. During random result verification, it was detected that the file might still be available, but that the content has been significantly altered to remove the detected PII. Upon the re-examination of the specified file, no PII was detected.

8.11 SUMMARY

While implementing a national monitoring system has been proven to be technically feasible, success depends on more than just the detection of vulnerabilities. Relevant stakeholders will have to work together to ensure the successful reduction of vulnerabilities and to increase the national security posture.

A full breakdown of role players is beyond the scope of this experiment, but ISPs will be key in achieving information security readiness as discussed previously. This is due to the fact that machines located on the national Internet infrastructure frequently make use of ISPs' infrastructure. When a query regarding the owner of the IP address is performed, it will resolve to the ISP and not to the owner. Only the ISPs will have information regarding the owner of the machine unless the machine in question provides a direct link to its owner.

The potential to use current security metrics on a national level has been demonstrated. While true that not all metrics could be assessed, the system can continually be

improved by following the PDCA process. Funding will always remain a consideration. Instead of attempting to solve all the problems, it should be considered that tracking the problem is already a step towards solving the problem.

The following chapter presents conclusions regarding the work performed in this study. The chapter will additionally also present potential future work that might be derived from the work performed in this study.

Stealing is stealing, whether you use a computer command or a crowbar, and whether you take documents, data or dollars.

Carmen M. Ortiz – Attorney

9

Conclusion

The research presented in this study has examined and collected information from 32 open and commercial data sources that could be used to obtain information related to national cyber security. The examination of these data sources and especially how they apply to the South African .co.za domain is believed to be the first study of its kind. Of the data sources evaluated in Chapter 4, 9 were selected for use in an experimental data fusion system in Section 5.6. The purpose of the system was to visualize the state of South Africa as seen from open and commercial datasets that are available to attackers. Data was collected over a two year period and resulted in the identification and geolocation of over a million-internet facing infrastructure devices in the South African domain. 88 Million potential vulnerabilities as well as over 2 million breached PII records were recorded during the course of this study.

9.1 Novel contributions and research outputs

This research presented in this study resulted in five novel contributions:

1. The adapted JDL model for use in the cyber domain on a national level was presented in Chapter 5.
2. The results of a detailed examination regarding data sources and their applicability to the South African .co.za domain as discussed in Chapters 4, 6 and 7.
3. A custom developed application that provides the ability to search for and validate detected PII in unstructured data sources was presented in Section 0.
4. Detection of PII through multiple search engines and open source APIs to augment the lack of information regarding the human component of the cyber environment was presented in Section 7.3.
5. A experimental system to visualize the results of the fusion process obtained from the adapted JDL model as described in Section 5.14.

A number of publications were produced during the course of this study and these are listed in Appendix D.

9.2 RESEARCH REVIEW

This section recaps what has been discussed in the research document by providing a brief summary of the purpose each chapter had.

Chapter 1 – The scope and aim of the research was presented.

Chapter 2 – Presented a review of national level cyber security policies and legislation with specific focus on desired outcomes and practical limitations such as information sharing.

Chapter 3 – Described information security concepts such as attack surfaces and the distinction between pro-active and re-active security implementations in order to highlight how existing data sources could contribute to increase national cyber security.

Chapter 4 – Presented the results from a evaluation of more than seventeen data sources that provide information relating to specific aspects of information security. The data sources selected had to contain data at a volume significant enough, that it could be applied at a national level.

Chapter 5 – Introduced an adapted JDL model for effective data fusion on a national level. The experimental system architecture is discussed with reference to the JDL model prescribed levels one to five. Source code and database layout are also included to indicate the relationships between entities and their properties.

Chapter 6 – Discussed the results of a case study on the infrastructure detected in the South African domain. The case study examined the dominant devices and software present in South Africa as well as known associated vulnerabilities.

Chapter 7 – Explored the detection and distribution of personally identifiable information in the South African domain. The data was presented in the experimental system first discussed in Chapter 6.

Chapter 8 – Analyzed the results obtained in the preceding chapters with a focus on the fusion component. The chapter examined the limitations of the current overall experiment and proposed potential future solutions and improvements.

Chapter 9 – Concludes by providing an overview of what was achieved in this study to meet the research objectives. A chronological layout of the topics presented in this research and aspects not explored in this study but worthy of future research is also presented.

9.3 RESEARCH OBJECTIVES

The three primary research objectives stated in Chapter 1 are revisited below:

1. In support of research objective one, the current status of cyber crime driving the need for national cyber security action were discussed. Technical aspects such as government responsibility, potential domain demarcation and previous cyber security strategy implementation failures were examined in Chapter 2. The role that open source information could provide to alleviate previously documented implementation difficulties was discussed in Chapter 3.
2. To address objective 2, an assessment of 32 data sources that could provide information relating to the attack surface of a nation was conducted in Chapter 4. Following the examination, 9 suitable data sources were identified and used in a JDL fusion system to pro-actively visualize national cyber security vulnerabilities. The architecture and model used for the fusion process are documented in Chapter 5, and the results of the infrastructure case study presented in Chapter 6.
3. The system described in Chapter 5 was suitably extended to provide the data breach detection capability stated by objective 3. A case study with the results of the extension of PII detection is available in Chapter 7.

Chapter 8 further discusses the limitations of the current fusion process for all stated objectives as well as potential solutions that will be addressed in future revisions of the system.

9.4 REFLECTION ON THE ACHIEVEMENT OF THE RESEARCH OBJECTIVES

The study evaluated the key criteria for information security readiness as described by the various international cyber security policies. Building on the information obtained, the study resulted in a functional prototype that visualizes a variety of vulnerabilities on a national level. The vulnerabilities visualized are not only on the device and software components, but on the human aspect as well with the visualization of detected PII. Data obtained for the system was all obtained through the use of third parties

reducing the chance of legal complications and reducing the need for significant custom scanning infrastructure development. Where custom developed software was used, it was clearly discussed. A secondary tool for the investigation of data breaches was also presented in Chapter 7. The main purpose of this tool is to alleviate the complexity involved with analyzing data breach information (Swart et al., 2013). The research presented has resulted in a number of publications both nationally and internationally as discussed in previous chapters.

9.5 FUTURE WORK

Prior chapters have discussed the results and contribution of this research. In conclusion however, it is the opinion of the author that the biggest stumbling blocks that remain in information security are those of effective visualization and clear legislation. For nearly every security flaw, a potential solution exists but has not been applied due to either ignorance or lack of awareness. A passionate community of information security researchers is available, often offering its services for free in the form of bug disclosures or vulnerability databases. However, legislation is unclear and discourages sharing of detected vulnerabilities to improve on the current situation, limiting their effectiveness. With effective and clear legislation researchers will be able to conduct increased research and development for the benefit of all, without fear of prosecution.

During the course of the study several future research areas were identified but not fully explored:

1. **Legal aspects of national infrastructure scanning in South Africa and internationally** – Significant legislation exists that could make information security research potentially illegal. This uncertainty inhibits effective information security research when in fact it should be encouraged at this point in time. This is not only a national problem but a international concern.
2. **How data breaches affect not only an individual company but a significant amount of other companies** – A large number of corporate email addresses detected in Chapter 7 were leaked from personal online services. It is thus clear that employees make use of workplace e-mail for personal business. Should a third party breach occur, the impact is thus not only limited to the victim company and the individual whose data was leaked. The employer of the individual affected is also potentially at increased risk due to the spear-phishing attacks that could follow.

3. **Identification of metrics to measure cyber security readiness of a country on a technical level** – The research presented has shown that a significant amount of information spanning a wide attack surface is available on a national level. Further exploration of quantification of these data sources could lead to an effective national preventative system.
4. **The use of machine learning to better detect vulnerabilities, personal information and drive by malware** – Current techniques of detecting personal information is limited and requires the ability to process available information in context. Vulnerabilities in systems can be identified by means of CVE libraries but in many instances require human verification; this could be addressed with effective machine learning techniques.
5. **Application of the algorithms and machine learning techniques identified in the adapted JDL model** – The potential for effective data fusion was presented in this research. While the results obtained are useful, significant additional fusion potential exists to more effectively identify entity relationships. Identifying the relationships between entities could lead to better prediction of future states on higher order levels in the JDL model. The electronic warfare research field has had a long history of effective data fusion. By examining the literature available, a best practice approach for information security might be identified for data fusion on a large scale.

9.6 CONCLUSION

Finally, this study by no means suggests that technical controls are the only solution to the current information security problem. However, good technical controls and visualization can allow decision makers the opportunity to make improved choices based on the best possible data available. Humans understand visual concepts significantly better than pages of text and while domain experts are often comfortable with copious amount of technical details, people governing decisions are often not domain experts at a technical level. The need for abstraction and distilling technical aspects into useful information for decision makers is thus a requirement even if it does detract from the granularity of the information. Information security stability will only be achieved with the co-operation of a multitude of organizations which in the end is operated by humans that first need to grasp the problems. Plohmann et al., (2011) highlights that while user education is the only real solution to the botnet problem, user awareness is also one of the most costly programs to implement.

References

Adeniran, T. V., & Johnston, K. A. *ICT utilisation within Experienced South African Small and Medium Enterprises. The Electronic Journal of Information Systems in Developing Countries,* 64(5):1-23, Feb 2014. ISSN 1681-4835.
URL http://www.ejisdc.org/ojs2/index.php/ejisdc/article/view/1152/531

Anand, A., Ramadurai, G., & Vanajakshi, L. *Data fusion based traffic density estimation and prediction. Journal of Intelligent Transportation Systems,* 18(4):367-378. Jul 2014. ISSN 1547-2442.
URL http://dx.doi.org/10.1080/15472450.2013.806844

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., Moore, T., & Savage, S. *Measuring the cost of cybercrime.* In **R. Böhme**., editor, *The economics of information security and privacy,* chapter 5, pages 265-300. Springer, Heidelberg, 2013. ISBN 978-3-642-39498-0.
URL http://link.springer.com/chapter/10.1007%2F978-3-642-39498-0_12

Anderson, R., & Moore, T. *The economics of information security. Science (New York, N.Y.), 314*(5799):610-613. Oct 2006. ISSN 1095-9203.
URL http://www.sciencemag.org/content/314/5799/610.short

Andrienko, G. L., & Andrienko, N. V. *Interactive maps for visual data exploration. International Journal of Geographical Information Science,* 13(4):355-374. Aug 2010. ISSN 1362-3087
URL http://dx.doi.org/10.1080/136588199241247

Assolini, F. *The tale of one thousand and one DSL modems.* Online, 1 October 2012. Last accessed: 2014/03/22.
URL http://securelist.com/blog/research/57776/the-tale-of-one-thousand-and-one-dsl-modems/

Aura, T., Kuhn, T. A., & Roe, M. *Scanning electronic documents for personally identifiable information.* In *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society WPES '04,* pages 41-50. ACM Press, New York, NY, USA, 2006.
URL http://doi.acm.org/10.1145/1179601.1179608

Babak, J., & Deviant, O. *Electronic locks - are really secure?!* Online, 2010. DeepSec, Vienna. Last Accessed: 2014/04/21.
URL https://www.youtube.com/watch?v=ZK0MfE7o4HU

Badawy, M. A., El-Fishawy, N., & Elshakankiry, O. *Vulnerability scanners capabilities for detecting windows missed patches: Comparative study.* In **Awad, A. I., Hassanien, A. E., Baba, K.,** editors, *Advances in Security of Information and Communication networks. Proceedings of the 1st Advances in security of information and communication networks, SECNET 2013,* pages 185-195. Springer, Berlin, Heidelberg, Sep 2013. ISBN 978-3-642-40597-6. doi: 10.1007/978-3-642-40597-6_16.
URL http://link.springer.com/chapter/10.1007%2F978-3-642-40597-6_16

Baker, J. C., Lachman, B. E., Frelinger, D. R., O'Connell, K. M., & Hou, A. C. *Mapping the risks: Assessing the homeland security implications of publicly available geospatial information, Rand Corporation.* Online, 2004. Last Accessed: 2013-08-22.
URL http://www.rand.org/pubs/monographs/MG142.html

Barclay, R. A. *Regulatory economics: Cybersecurity—Who cares? threat and apathy worldwide, outlook uncertain. Natural Gas & Electricity,* 30(6):30-32. Jan 2014. ISSN 1545-7907.
URL http://onlinelibrary.wiley.com/doi/10.1002/gas.21738/full

Barnum, S. *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).* Online, 2013. Last Accessed: 2014/05/23.
URL http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0.pdf

Barth, A., Rubinstein, B. I., Sundararajan, M., Mitchell, J. C., Song, D., & Bartlett, P. L. *A learning-based approach to reactive security.* In **Sion, R.,** Editor, *Financial cryptography and data security,* pages 192-206. Springer, Berlin, Heidelberg, 2010. ISBN 978-3-642-14577-3.
URL http://dx.doi.org/10.1007/978-3-642-14577-3_16

Baskerville, R., Spagnoletti, P., & Kim, J. *Incident-centered information security: Managing a strategic balance between prevention and response. Information & Management,* 51(1):138-151. Jan 2014. ISSN 0378-7206.
URL http://dx.doi.org/10.1016/j.im.2013.11.004

Bass, T. *Intrusion detection systems and multisensor data fusion. Communications of the ACM,* 43(4):99-105. Apr 2000. ISSN 0001-0782.
URL http://dx.doi.org/10.1145/332051.332079

Beaudoin, L., Gregoire, M., Lagadec, P., Lefebvre, J., Luiijf, E., & Tolle, J. *Coalition network defence common operational picture.* Conference paper, Fraunhofer Society, Wachtberg, Germany, Nov 2010.
URL www.dtic.mil/get-tr-doc/pdf?AD=ADA584050

Bellovin, S. M., Bradner, S. O., Diffie, W., & Landau, S. *Can it really work? problems with extending EINSTEIN 3 to critical infrastructure. Harvard National Security Journal,* 3:1-34. Jan 2012. ISSN 2153-1358.
URL http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Bellovin_Bradner_Diffie_Landau_Rexford.pdf

Benjamin, V., & Chen, H. *Securing cyberspace: Identifying key actors in hacker communities.* In *Intelligence and Security Informatics (ISI), 2012 IEEE International Conference.* 11-14 June 2012. Washington, DC, USA.
URL http://dx.doi.org/10.1109/ISI.2012.6283296

Berghel, H. *Better-than-nothing security practices. Communications of the ACM, 50*(8):15-18. ISSN 0001-0782.
URL http://dx.doi.org/10.1145/1278201.1278222

Bertini, E., & Lalanne, D. *Surveying the complementary role of automatic data analysis and visualization in knowledge discovery.* In *Proceedings of the ACM SIGKDD Workshop on Visual Analytics and Knowledge Discovery: Integrating Automated Analysis with Interactive Exploration,* VAKD '09, pages 12-20. ACM, New York, NY, USA, 2009.
URL http://dx.doi.org/10.1145/1562849.1562851

Bhatia, S., Hussaini, A., Navalakha, S., & Zhou, M. *MIS 510: Cyber analytics project.* Grad student report, Arizona University, Arizona, USA, 2014.
URL http://ai.arizona.edu/mis510/syllabus/ProjectResources/sample_projects/2014%20Spring/Cybersecurity/Session1/14/Report.pdf

Bianco, D. *The pyramid of pain.* Online, March 2013. Last accessed: 2014/01/26. URL http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Bishop, M. *What is computer security? Security & Privacy, IEEE, 1*(1):67-69, 2003. ISSN 1540-7993.
URL http://dx.doi.org/10.1109/MSECP.2003.1176998

Blasch, E. *Enhanced air operations using JView for an air-ground fused situation awareness udop.* In *Digital Avionics Systems Conference (DASC) 2013 IEEE/AIAA 32nd,* pages 5A5-1-5A5-11. East Syracuse, NY, 5-10 Oct 2013. ISSN 2155-7195 doi: 10.1109/DASC.2013.6712597.
URL http://dx.doi.org/10.1109/DASC.2013.6712597

Blasch, E., & Plano, S. *JDL level 5 fusion model: User refinement issues and applications in group tracking.* In **Kadar, I.,** editor, *Signal Processing, Sensor Fusion, and Target Recognition XI*, pages 270-279. SPIE, Orlando, FL, 2002.
URL http://dx.doi.org/10.1117/12.477612

Bojinov, H., Michalevsky, Y., Nakibly, G., & Boneh, D. *Mobile device identification via sensor fingerprinting.* In *Corr*, 1408.1416:1-14, 2014.
URL http://arxiv.org/abs/1408.1416

Bonkoski, A., Bielawski, R., & Halderman, A. *Illuminating the security issues surrounding lights-out server management.* In *Proceedings of the 7th USENIX Workshop on Offensive Technologies, WOOT '13*, pages 1-9. Washington, D.C. USENIX, Berkeley, CA, 2013.
URL https://www.usenix.org/conference/woot13/workshop-program/presentation/Bonkoski

Bossler, A. M., & Holt, T. J. *Patrol officers' perceived role in responding to cybercrime.* In *Policing: An International Journal of Police Strategies & Management,* 35(1):165-181, 2012. ISSN 1363-951X.
URL http://dx.doi.org/10.1108/13639511211215504

Breindl, Y., & Kuellmer, B. *Internet content regulation in france and germany: Regulatory paths, actor constellations, and policies.* In *Journal of Information Technology & Politics,* 10(4):369-388, 2013. ISSN 1933-169X.
URL http://dx.doi.org/10.1080/19331681.2013.803947

Brenner, S. W. *Distributed security: Moving away from reactive law enforcement. International Journal of Communications Law & Policy,* 9:1-40, 2004.
ISSN 1439-6262.
URL http://ssrn.com/abstract=623283

Broadhurst, R. *Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies & Management,* 29(3):408-433.
ISSN 1363-951X.
URL http://dx.doi.org/10.1108/13639510610684674

Brown, G., Carlyle, M., Salmeron, J., & Wood, K. *Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses.* In **Greenberg, H., & Smith, J.**, editors, *Tutorials in Operations Research: Emerging Theory, Methods, and Applications. Institute for Operations Research and Management Science*, Chapter 4, pages 102-123. Hanover, MD. 2005
URL http://pubsonline.informs.org/doi/pdf/10.1287/educ.1053.0018

Butler, J., & Lachow, I. *Multilateral approaches for improving global security in cyberspace. Georgetown Journal of International Affairs,* Special issue 2012:gj127, 2012. ISSN 1526-0054

Buttyán, L., Gessner, D., Hessler, A., & Langendoerfer, P. *Application of wireless sensor networks in critical infrastructure protection: Challenges and design options [security and privacy in emerging wireless networks]. Wireless Communications, IEEE,* 17(5):44-49, October 2014. ISSN 1536-1284.
URL http://dx.doi.org/10.1109/MWC.2010.5601957

Cadariu, M. *Tracking known security vulnerabilities in third-party components.* Master's thesis, Delft University of Technology, Aug 2014.
URL http://repository.tudelft.nl/assets/uuid:504b4d73-c4ab-4e5e-bcaf-ca6d2ff7347b/thesis.pdf

Caicedo, C. E., Joshi, J. B., & Tuladhar, S. R. *IPv6 security challenges. IEEE Computer,* 42(2):36-42, Feb 2009. ISSN 0018-9162.
URL http://dx.doi.org/10.1109/MC.2009.54

Card, S., Mackinlay, J., & Shneiderman, B. *Readings in information visualization: Using vision to think*. Morgan Kaufmann, Massachusetts, Illustrated edition, February 1999. ISBN 978-1558605336.

Carr, J. *Inside cyber warfare: Mapping the cyber underworld* (Illustrated ed.). O'Reilly Media, Inc, Massachusetts, United States, December 2011. ISBN 978-1449310042.

Caselli, M., Hadžiosmanović, D., Zambon, E., & Kargl, F. *On the feasibility of device fingerprinting in industrial control systems.* In *Critical information infrastructures security, 8th International Workshop CRITIS 2013,* pages 155-166. Springer International Publishing, Switzerland. ISBN 978-3-319-03963-3
ISSN 0302-9743.
URL http://dx.doi.org/10.1007/978-3-319-03964-0_14

Castanedo, F. *A review of data fusion techniques*. *The Scientific World Journal,* 2013(704504):1-19, Sept 2013. ISSN 1537-744X.
URL http://dx.doi.org/10.1155/2013/704504

Cavelty, M. D. *Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. Science and Engineering Ethics,* 20(3):701-715, Sept 2014. ISSN 1471-5546.
URL http://dx.doi.org/10.1007/s11948-014-9551-y

Cavusoglu, H., & Raghunathan, S. *Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge. Software Engineering, IEEE Transactions On,* 33(3):171-185, March 2007. ISSN 0098-5589.
URL http://dx.doi.org/10.1109/TSE.2007.26

Center for Strategic and International Studies. *Net losses: Estimating the global cost of cybercrime.* Online, 2014. Last accessed, 2014/07/17.
URL http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Chen, J., Díaz, M., Llopis, L., Rubio, B., & Troya, J. M. *A survey on quality of service support in wireless sensor and actor networks: Requirements and challenges in the context of critical infrastructure protection. Journal of Network and Computer Applications,* 34(4):1225-1239, Jul 2011. ISSN 1084-8045.
URL http://dx.doi.org/10.1016/j.jnca.2011.01.008

Christey, S., & Marion, B. *Buying into the bias: Why vulnerability statistics suck.* Online, 2013. BlackHat, Las Vegas, USA. Last accessed: 2014-12-23.
URL https://media.blackhat.com/us-13/US-13-Martin-Buying-Into-The-Bias-Why-Vulnerability-Statistics-Suck-Slides.pdf

Clemente, D.. *Cyber security and global interdependence: What is critical?* Chatham House, Royal Institute of International Affairs, May 2013, 40 pages.
ISBN 978-1862032781.

Coburn, T. *The federal government's track record on cybersecurity and critical infrastructure.* Online, February 2014. Last accessed: 2014-12-01
URL http://www.hsgac.senate.gov/download/the-federal-governments-track-record-on-cybersecurity-and-critical-infrastructure

Cody, B. *My arduino can beat up your hotel room lock.* Online, 2012. BlackHat, Las Vegas, USA. Last accessed:, 2014/05/25.
URL https://media.blackhat.com/bh-us-12/Briefings/Brocious/BH_US_12_Brocious_Hotel_Key_Slides.pdf

Conrad, B., & Shirazi, F. *Survey on tor and I2P.* In *Proceedings of the Ninth International Conference on Internet Monitoring and Protection ICIMP 2014,* pages 22-28. IARIA XPS, Paris, France, 2014. ISSN 2308-3980. ISBN 978-1-61208-362-9.

Cui, A., Kataria, J., & Stolfo, S. J. *Revisiting the myth of cisco IOS diversity: Recent advances in reliable shellcode design. Information Management & Computer Security,* 21(2):121-138, Jan, 2013. ISSN 0968-5227.
URL http://dx.doi.org/10.1108/IMCS-09-2012-0046

Culnan, M. J., & Bies, R. J. *Consumer privacy: Balancing economic and justice considerations. Journal of Social Issues,* 59(2):323-342, July 2003. ISSN 1540-4560.
URL http://dx.doi.org/10.1111/1540-4560.00067

Dainotti, A., Squarcella, C., Aben, E., Claffy, K. C., Chiesa, M., Russo, M., & Pescapé, A. *Analysis of country-wide internet outages caused by censorship.* In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference,* pages 1-18. ACM, New York, NY, USA, 2011. ISBN 978-1-4503-1013-0. URL http://dx.doi.org/10.1145/2068816.2068818

Dalal, A. S. Shadow administrative constitutionalism and the creation of surveillance culture. *Michigan State Law Review,* 2014(1):58-138, 2014. ISSN 2328-3068. URL http://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1002&context=lr

Davey, J., Mansmann, F., Kohlhammer, J., & Keim, D. *Visual analytics: Towards intelligent interactive internet and security solutions.* In *The future Internet Assembly 2012: From Promises to Reality,* pages 93-104. Springer, Berlin, Heidelberg, 2012. ISBN 978-3-642-30241-1. URL http://dx.doi.org/10.1007/978-3-642-30241-1_9

De Bruijne, M., & Van Eeten, M. *Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment. Journal of Contingencies and Crisis Management,* 15(1):18-29, March 2007. ISSN 1468-5973. URL http://onlinelibrary.wiley.com/doi/10.1111/j.1468-5973.2007.00501.x/pdf

De Kunder, M. *Geschatte grootte van het geïndexeerde world wide web.* Thesis, University of Tilburg, March 2007. Last accessed: 2014/02/21. URL http://www.dekunder.nl/Media/Scriptie%20Maurice%20de%20Kunder%20-%20Grootte%20geindexeerde%20web.pdf

De Souza, C. *National cyber security: The responsibility of all sectors.* Master's thesis, UTICA College, Department Cybersecurity, New York, USA, 2014. URL http://search.proquest.com/docview/1527125694

Delort, J. *Hierarchical cluster visualization in web mapping systems.* In *Proceedings of the 19th International Conference on World Wide Web,* pages 1241-1244. ACM, New York, NY, USA, 2010. ISBN 978-1-60558-799-8. URL http://dx.doi.org/10.1145/1772690.1772892

Demchak, C. C., & Dombrowski, P. *Rise of a cybered westphalian age. Strategic Studies Quarterly,* 5(1)32-61, 2011. ISSN 1936-1815.
URL http://www.dtic.mil/dtic/tr/fulltext/u2/a537560.pdf

DeNardis, L. *The emerging field of internet governance. Yale Information Society Project Working Paper Series,* 2010.
URL http://dx.doi.org/10.2139/ssrn.1678343

Dlamini, Z., Taute, B., & Radebe, J. *Framework for an african policy towards creating cyber security awareness.* In *Proceedings of the First IFIP TC9/TC11 South African Cyber Security Awareness Workshop (SACSAW) 2011,* pages 15-31.
URL http://researchspace.csir.co.za/dspace/bitstream/10204/5163/1/Dlamini_2011.pdf

Doherty, M., & Hawkey, K. *Problematic computer crime laws in Canada.* Online, 2014. Last Accessed: 2014/02/26.
URL https://hashbang.ca/wp-content/uploads/2013/11/report1.pdf

Doupé, A., Cova, M., & Vigna, G. *Why Johnny can't pentest: An analysis of black-box web vulnerability scanners.* In *Detection of Intrusions and Malware, and Vulnerability Assessment, 7th International Conference, DIMVA 2010,* pages 111-131. Springer, Berlin, Heidelberg, 2010. ISBN 978-3-642-14215-4.
URL http://dx.doi.org/10.1007/978-3-642-14215-4_7

Durumeric, Z., Wustrow, E., & Halderman, J. A. *ZMap: Fast internet-wide scanning and its security applications.* In *Proceedings of the 22nd USENIX Security Symposium,* pages 605-619. Washington DC, USA, 2013.
URL https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/durumeric

Endsley, M. R. *Toward a theory of situation awareness in dynamic systems. Human Factors: The Journal of the Human Factors and Ergonomics Society,* 37(1):32-64. ISSN 0018-7208. doi: 10.1518/001872095779049543.

Fahmy, H. M., & Ghoneim, S. A. *PhishBlock: A hybrid anti-phishing tool.* In *Communications, Computing and Control Applications (CCCA), 2011 International Conference On,* pages 1-5. 2001. IEEE.
URL http://dx.doi.org/10.1109/CCCA.2011.6031523

Falessi, N., Gavrila, R., Klejnstrup, R. & Moulinos, K. *National cyber security strategies: An implementation guide.* Online, 2012. Last Accessed: 2014/01/13.
URL http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

Falliere, N., Murchu, L. O. & Chien, E. *W32. stuxnet dossier.* Online, Feb 2011. Last accessed, 2014/0525.
URL http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Feaver, P., & Geers, K. *"When the urgency of time and circumstances clearly does not permit...": Predelegation in nuclear and cyber scenarios.* In **Goldman, E.O., Arquilla, J.,** editors, *Cyber Analogies*, pages 33-45, 2014. Monterey, California, Naval Postgraduate School.
URL https://calhoun.nps.edu/handle/10945/40037

Fischer, E. N., Dudding, C. M., Engel, T. J., Reynolds, M. A., Wierman, M. J., Mordeson, J. N., & Clark, T. D. *Explaining variation in state involvement in cyber attacks: A social network approach.* In *Social networks: A framework of computational intelligence,* pages. 63-74. Springer, Manhattan, New York. ISBN 978-3-319-02993-1. doi:10.1007/978-3-319-02993-1_4.

Florêncio, D., & Herley, C. *Sex, lies and cyber-crime surveys.* In **Schneier, B.,** editor, *Economics of information security and privacy III,* pages 35-53, 2013. Springer, Manhattan, New York. ISBN 978-1-4614-1981-5. doi:10.1007/978-1-4614-1981-5_3

Ford, R. *Law and borders. Alabama Law Review,* 64:123-139, 2013. ISSN 0002-4279.
URL http://www.law.ua.edu/pubs/lrarticles/Volume%2064/Issue%201/4%20Ford%20123%20-%20139.pdf

Ford, T., Hofmann, M., & Bankston, K. *The big chill: Legal landmines that stifle security research and how to disarm them*. Online, 2014. Black Hat, Las Vegas, USA. Last Accessed: 2014-08-17.
URL https://www.blackhat.com/docs/us-14/materials/us-14-Ford-Big-Chill.pdf

Fran, B. *RFID hacking.* Online, 2013. Black Hat, Las Vegas, USA. Last Accessed: 2014/05/25.
URL https://media.blackhat.com/us-13/US-13-Brown-RFID-Hacking-Live-Free-or-RFID-Hard-Slides.pdf

Gagnon, M. N., Truelove, J., Kapadia, A., Haines, J., & Huang, O. *Towards Net-Centric Cyber Survivability for Ballistic Missile defense.* In **Giese, H.,** editor, *Architecting critical systems, First International Symposium, ISARCS 2010,* pages125-141, 2010. Springer, Berlin, Heidelberg. ISBN 978-3-642-13556-9.
URL http://dx.doi.org/10.1007/978-3-642-13556-9_8

Gasper, P. D. *Cyber threat to critical infrastructure-2010-2015.* Conference Presentation Information & Cyberspace Symposium, Fort Leavenworth, Kansas, September 2008.
URL http://usacac.army.mil/cac2/cew/repository/papers/Cyber_Threat_to_CI.PDF

Geer, D. *Cybersecurity and national policy. Harvard National Security Journal,* 1:203-215, Jan 2011. ISSN 2153-1358.
URL http://harvardnsj.org/2011/01/cybersecurity-and-national-policy/

Geer, D., & Archer, J. *Stand your ground. IEEE Security & Privacy,* 10(4):96, Jul 2012. ISSN 1540-7993.
URL http://dx.doi.org/10.1109/MSP.2012.109

Giacobe, N. A. *Application of the JDL data fusion process model for cyber security.* In **Braun, J.,** editor, *SPIE 7710, Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications,* pages 77100R-77100R-10, April 2010.
URL http://dx.doi.org/10.1117/12.850275

Giacobe, N. A. *Data fusion in cyber security: First order entity extraction from common cyber data.* In **Ternovskiy, I. V., & Chin, P.,** editors, *SPIE 8408, Cyber Sensing,* pages 84080E-84080E-7, May 2012.
URL http://dx.doi.org/10.1117/12.919379

Giacobe, N. A. *Measuring the effectiveness of visual analytics and data fusion techniques on situation awareness in cyber-security.* PhD thesis, Pennsylvania State University, Pennsylvania, USA. 12 December 2012.
URL https://etda.libraries.psu.edu/paper/17537/16009

Giglietto, F., Rossi, L., & Bennato, D. *The open laboratory: Limits and possibilities of using facebook, twitter, and YouTube as a research data source. Journal of Technology in Human Services, 30*(3-4):145-159, Oct 2012. ISSN 1522-8991.
URL http://dx.doi.org/10.1080/15228835.2012.743797

Gilad, Y., Herzberg, A., & Shulman, H. *Off-path hacking: The illusion of challenge-response authentication. Security & Privacy, IEEE, 12*(5):68-77, October 2014. ISSN 1540-7993.
URL http://dx.doi.org/10.1109/MSP.2013.130

Glassman, M., & Kang, M. J. *Intelligence in the internet age: The emergence and evolution of open source intelligence (OSINT). Computers in Human Behavior, 28*(2):673-682, March 2012.
URL http://dx.doi.org/10.1016/j.chb.2011.11.014

Goldsmith, J. L., & Wu, T. *Who controls the internet? Illusions of a borderless world.* Oxford University Press, New York, 240 pages, June 2008. ISBN 978-0195340648.

Goldstuck, A. *Internet matters: The Quiet Engine of the South African Economy.* Online, 2013/10/23. Last Accessed: 2014-01-23.
URL http://www.internetmatters.co.za/report/ZA_Internet_Matters.pdf

Goodin, D. *Dear Asus router user: You've been pwned, thanks to easily exploited flaw.* Online, 2014/02/17. Last Accessed: 2014-09-23.
URL http://arstechnica.com/security/2014/02/dear-asus-router-user-youve-been-pwned-thanks-to-easily-exploited-flaw/

Gopal, R., Marsden, J. R., & Vanthienen, J. *Information mining—Reflections on recent advancements and the road ahead in data, text, and media mining. Decision Support Systems, 51*(4):727-731, November 2011. ISSN 0167-9236.
URL http://dx.doi.org/10.1016/j.dss.2011.01.008

Grady, D. *The vision thing: Mainly in the brain. Discover magazine, 14*(6):56-66, June 1993. ISSN 0274-7529.
URL http://discovermagazine.com/1993/jun/thevisionthingma227

Gritzalis, D. *Open source intelligence produced from online social networks: A proactive cyber-defense tool.* In *Proceedings of the 13th European Conference on Cyber Warfare and Security, Keynote Address,* July 2014. ISBN 978-1-910309-26-1
URL http://www.cis.aueb.gr/Publications/ECCWS-2014%20Keynote%20address.pdf

Gujrathi, S. *Heartbleed bug: An OpenSSL heartbeat vulnerability. International Journal of Computer Science and Engineering,* 2(5):61-64, 2014. ISSN 2319-7323.
URL http://www.ijcseonline.org/pub_paper/IJCSE-00277.pdf

Hall, D. L., & Llinas, J. *An introduction to multisensor data fusion. Proceedings of the IEEE,* 85(1):6-23, Jan 1997. ISSN 0018-9219.
URL http://dx.doi.org/10.1109/5.554205

Hall, D. L., McNeese, M. D., Hellar, D. B., Panulla, B. J., & Shumaker, W. *A cyber infrastructure for evaluating the performance of human centered fusion.* In *Information Fusion, 2009. FUSION'09. 12th International Conference On,* pages 1257-1264, July 2009. ISBN 978-0-9824-4380-4.

Hammer, R. U., J. *Inside-out vulnerabilities, reverse shells.* Online, May 2006. Last Accessed: 2014/02/13.
URL http://www.sans.org/reading-room/whitepapers/covert/inside-out-vulnerabilities-reverse-shells-1663

Hansen, A. *Research note protecting critical infrastructure.* Online, Jun 2012. Last Accessed: 2014/03/01.
URL http://anniesearle.com/web-services/Documents/ResearchNotes/ASA_ ResearchNote_ProtectingCriticalInfrastructure_June2012.pdf

Harris, A., Goodman, S., & Traynor, P. *Privacy and Security Concerns Associated with Mobile Money Applications in Africa. Washington Journal Of Law, Technology & Arts,* 8(3):245-264, 2013. ISSN 2157-2534.
URL https://files.law.washington.edu/other/MobileMoney/public/ HarrisGoodmanTraynor.pdf

Hart, M., Manadhata, P., & Johnson, R. *Text classification for data loss prevention.* In **Fischer-Hübner, S., Hopper, N.,** editors, *11th International Symposium 2011,* pages 18-37, 2011. Springer, Berlin, Heidelberg. ISBN 978-3-642-22263-4. URL http://dx.doi.org/10.1007/978-3-642-22263-4_2

Hathaway, M. *Cyber readiness index 1.0.* Online, 2013. Last Accessed, 2013/12/27. URL http://belfercenter.hks.harvard.edu/publication/23607/cyber_readiness_index_10.html

Hayes, J., & Bodhani, A. *Cyber security: Small firms under fire. Engineering & Technology,* 8(6):80-83, July 2013. ISSN 1750-9637. URL http://dx.doi.org/10.1049/et.2013.0614

Herzog, S. *Revisiting the estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security,* 4(2):4, August 2011. ISSN 1944-0464

Hofmeyr, S., Moore, T., Forrest, S., Edwards, B., & Stelle, G. *Modeling internet-scale policies for cleaning up malware.* In **Schneier, B.,** editor, *Economics of information security and privacy III,* pages 149-170, 2013. Springer, Berlin, Heidelberg. ISBN 978-1-4614-1981-5. doi:10.1007/978-1/4614/-1981-5_7.

Holden-Rhodes, J. F. *Sharing the secrets: Open source intelligence and the war on drugs.* Praeger, London, Westport, 256 Pages, January 1997. ISBN 978-0275954543.

Holm, H., Sommestad, T., Almroth, J., & Persson, M. *A quantitative evaluation of vulnerability scanning. Information Management & Computer Security,* 19(4)231-247, 2011. ISSN 0968-5227. URL http://dx.doi.org/10.1108/09685221111173058

Homeland Security. *National Infrastructure Protection Plan 2013, partnering for critical infrastructure security and resilience.* Online, February 2014. Last Accessed, 2014/04/22. URL http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf

Hudaib, A. A. Z. *DNS advanced attacks and analysis. International Journal of Computer Science and Security (IJCSS),* 8(2):63, 2014. ISSN 1985-1553. URL http://www.cscjournals.org/manuscript/Journals/IJCSS/volume8/Issue2/IJCSS-905.pdf

Hughes, R. J., Nordholt, J. E., McCabe, K. P., Newell, R. T., Peterson, C. G., & Somma, R. D. *Network-centric quantum communications with application to critical infrastructure protection,* 7 pages, May 2013. URL http://arxiv.org/abs/1305.0305

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.* In **Armistead, L.,** Editor, *Proceedings of the 6th International Conference on Informtion Warfare and Security,* pages 113-124, 2011. ISBN 19066389926.

Independent Security Evaluators. *Exploiting SOHO routers.* Online, 2014. Last Accessed, 2014/07/29. URL https://securityevaluators.com/knowledge/case_studies/routers/soho_router_hacks.php

Independent Security Evaluators. *SOHO network equipment ...and the implications of a rich service set.* Online, 2013. Last Accessed: 2014/07/28. URL https://securityevaluators.com/knowledge/case_studies/routers/soho_techreport.pdf

Invernizzi, L., Comparetti, P. M., Benvenuti, S., Kruegel, C., Cova, M., & Vigna, G. *Evilseed: A guided approach to finding malicious web pages.* In *Security and Privacy (SP), 2012 IEEE Symposium On,* pages 428-442, 2012. IEEE Computer Society, Washington, DC, USA. ISBN 978-0-7695-4681-0. URL http://dx.doi.org/10.1109/SP.2012.33

Irwin, B. V. W. *A framework for the application of Network Telescope Sensors in a global IP network.* PhD thesis, Rhodes University, Grahamstown, South Africa, 2011. URL http://www.academia.edu/1572544/a_framework_for_the_application_of_network_telescope_sensors_in_a_global_ip_network

Jacobs, P., Arnab, A., & Irwin, B. *Classification of security operation centers.* In *Information Security for South Africa,* pages 1-7, 2013.
URL http://dx.doi.org/10.1109/ISSA.2013.6641054

Jansen, R., Tschorsch, F., Johnson, A., & Scheuermann, B. *The sniper attack: Anonymously deanonymizing and disabling the tor network.* In *Network and Distributed Systems Security Symposium (NDSS),* 15 pages, 2014.
URL http://www.nrl.navy.mil/itd/chacs/sites/edit-www.nrl.navy.mil.itd.chacs/files/pdfs/13-1231-3743.pdf

Jansen, W. *Directions in security metrics research.* DIANE Publishing, Darby, Pennsylvania, USA, illustrated edition, 21 pages, 2010. ISBN 1437924514.

Jaquith, A. *Security metrics: Replacing fear, uncertainty, and doubt.* Addison-Wesley Professional, Boston, USA, 1st edition, 336 pages, April 2007. ISBN 9780321349989.

Jin, X., Lin, C., Luo, J., & Han, J. *A data mining-based spam detection system for social media networks.* In *Proceedings of the VLDB Endowment,* 4(12):1458-1461, 2011.
URL http://www.vldb.org/pvldb/vol4/p1458-jin.pdf

Johnson, T. A. *Forensic computer crime investigation,* CRC Press, Mortimer House, London, UK, 1st edition, 336 pages, September 2005. ISBN 0824724356.

Kachhadiya, R., & Benoist, E. *Development of the security framework based on OWASP ESAPI for JSF2. 0.* Online, 2013. Last Accessed: 2013/11/17.
URL https://www.owasp.org/index.php/OWASP_EJSF_Project

Kara, A. M., Binsalleeh, H., Mannan, M., Youssef, A., & Debbabi, M. *Detection of malicious payload distribution channels in DNS.* In *Communications (ICC), 2014 IEEE International Conference on,* pages 853-858, June 2014.
URL http://dx.doi.org/10.1109/ICC.2014.6883426

Karaklajić, D., Schmidt, J., & Verbauwhede, I. *Hardware designer's guide to fault attacks.* In *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on,* 21(12):2295-2306, February 2013. IEEE Circuits and Systems Society. ISSN 1063-8210.
URL http://dx.doi.org/10.1109/TVLSI.2012.2231707

Khaleghi, B., Khamis, A., Karray, F. O., & Razavi, S. N. *Multisensor data fusion: A review of the state-of-the-art*. In *Information Fusion,* 14(1):28-44, October 2013. Elsevier Science Publishers, Amsterdam, The Netherlands. ISSN 1566-2535. URL http://dx.doi.org/10.1016/j.inffus.2011.08.001

Kim, Z. *Researchers hack building control system at google australia office.* Online, 2013. Last Accessed: 2014/05/02. URL http://www.wired.com/2013/05/googles-control-system-hacked/

Kinder-Kurlanda, K., & Weller, K. *I always feel it must be great to be a hacker!: The role of interdisciplinary work in social media research*. In *Proceedings of the 2014 ACM Conference on Web Science,* pages 91-98, 2014. ACM, New York, NY, USA. ISBN 978-1-4503-2622-3. URL http://doi.acm.org/10.1145/2615569.2615685

Klimburg, A. *Mobilising cyber power. Survival,* 53(1):41-60, 2011. Routledge, Mortimer Street, London, UK. ISSN 0039-6338. URL http://dx.doi.org/10.1080/00396338.2011.555595

Klimburg, A. *National cyber security framework manual* Online, 2014. Last Accessed, 2014/12/02. URL http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport

Kohno, T., Broido, A., & Claffy, K. C. *Remote physical device fingerprinting.* In *Dependable and Secure Computing, IEEE Transactions On,* pages 93-108, May 2005. IEEE. ISBN 0-7695-2339-0. ISSN 1081-6011. URL http://dx.doi.org/10.1109/SP.2005.18

Kornmaier, A., & Jaouën, F. *Beyond technical data - a more comprehensive situational awareness fed by available intelligence information.* In *the 2014 6TH International Conference On Cyber Conflict (CYCON 2014),* pages 139-154, June 2014. IEEE. ISBN 978-9949-9544-0-7. ISSN 2325-5366. URL https://www.ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2014.pdf

Kotulic, A. G., & Clark, J. G. *Why there aren't more information security research studies. Information & Management,* 41(5):597-607, May 2004. ISSN 0378-7206. URL http://dx.doi.org/10.1016/j.im.2003.08.001

Krausz, M., & Walker, J. *The true cost of information security breaches and cyber crime.* IT Governance Publishing, 2013, 73 pages. ISBN 1849284962.

Krishnamurthy, B. Privacy leakage on the internet. Online, 2010. Last Accessed, 2014/01/10.
URL https://www.ietf.org/proceedings/77/slides/plenaryt-5.pdf

Kshetri, N. *Simple economics of cybercrime and the vicious circle.* In *The global cybercrime industry,* pages 35-55. Springer, Berlin, Heidelberg, 2010. ISBN 978-3-642-11522-6. doi: 10.1007/978-3-642-11522-6_2.

Kwon, J., & Johnson, M. E. *Proactive versus reactive security investments in the healthcare sector. Mis Quarterly,* 38(2):451-471, June 2014. ISSN 0276-7783. URL http://dl.acm.org/citation.cfm?id=2638645.2638652

Kyobe, M., Matengu, S., Walter, P., & Shongwe, M. *Factors inhibiting recognition and reporting of losses from cyber-attacks: The case of government departments in the western cape province of south africa.* In **Salmon, D.,** editor, *the 6th European Conference on Information Management and Evaluation,* pages 159-167. Academic Conferences, London, UK, 2012. ISBN 1908272651.

Larkin, B. D. *Note: Some revelatory breaches of security.* Online, 2014. Last Accessed, 2014/11/02.
URL http://www.learnworld.com/DESIGN/JPD/JN002=DD.136E=2013.12.11.SomeRevelatoryBreachesOfSecurity.pdf

LeBlanc, D., & Howard, M. *Writing Secure Code.* Microsoft Press, December 2002, 800 pages. ISBN 9780735617223.

Leverett, E. P. *Quantitatively Assessing and Visualising Industrial System Attack Surfaces.* University of Cambridge, Darwin College, June 2011.
URL http://www.scadaexposure.com/library/BH_US12-Leverett-Industrial.pdf

Lewis, J. *National perceptions of cyber threats. Strategic Analysis,* 38(4):566-576. ISSN 1754-0054.
URL http://dx.doi.org/10.1080/09700161.2014.918445

Lewis, R., Louvieris, P., Abbott, P., Clewley, N., & Jones, K. *Cybersecurity information sharing: A framework for sustainable information security management in UK SME supply chains.* In *Proceedings of the European Conference on Information Systems (ECIS) 2014,* pages 15-23. AIS Electronic Library, 2014. ISBN 978-0-9915567-0-0.

Luiijf, E., Besseling, K., & De Graaf, P. *Nineteen national cyber security strategies. International Journal of Critical Infrastructures,* 9(1/2):3-31, 2013. ISSN 1741-8038.
URL http://dx.doi.org/10.1504/IJCIS.2013.051608

Malone, T. W., & Klein, M. *Harnessing collective intelligence to address global climate change. Innovations: Technology, Governance, Globalization,* 2(3):15-26, 2007. ISSN 1558-2485.

Mandiant, International. *Mandiant, APT1 report.* Online, 2013. Last Accessed, 2014/0525.
URL http://www.intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Mao, J., Li, P., Li, K., Wei, T., & Liang, Z. *BaitAlarm: Detecting phishing sites using similarity in fundamental visual features*. In *Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference On,* pages 790-795.
URL http://dx.doi.org/10.1109/INCoS.2013.151

Marty, R. *Applied security visualization* (Illustrated ed.). Boston, USA: Addison-Wesley Professional, 2009, 552 pages. ISBN 0-321-51010-0

McDonald, G., Murchu, L. O., Doherty, S., & Chien, E. *Stuxnet 0.5: The missing link. Symantec Report*. Online, February 2013. Last Accessed, 2014/05/03.
URL http://www.symantec.com/connect/blogs/stuxnet-05-missing-link

McGuire, M., & Dowling, S. *Cyber crime: A review of the evidence. Summary of Key Findings and Implications. Home Office Research Report, 75.* Online, October 2013. Last Accessed, 2014/01/07.
URL https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

Meier, S., & Heidmann, F. *Too many markers, revisited.* In *Proceeding of the 14th International Conference on Computational Science and its Applications,* pages 121-125. IEEE, July 2014. doi: 10.1109/ICCSA.2014.31.

Mirowski, L., Hartnett, J., & Williams, R. *An RFID attacker behavior taxonomy. Pervasive Computing, IEEE,* 8(4):79-84. IEEE Computer Society. ISSN 1536-1268.
URL http://dx.doi.org/10.1109/MPRV.2009.68

MITRE. *Making security measureable.* Online, 2013. Last Accessed, 2014/02/26.
URL http://measurablesecurity.mitre.org/

Moore, H. *Security flaws in universal plug and play: Unplug. don't play*. Online, Jan 2013. Last Accessed, 2014/11/16.
URL https://community.rapid7.com/community/infosec/blog/2013/01/29/security-flaws-in-universal-plug-and-play-unplug-dont-play

Moore, T., & Anderson, R. *Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research.* In **Peitz, M., Waldfogel, J.,** editors, *The Oxford Handbook of the Digital Economy,* pages – , November 2012. Oxford Univeristy Press. ISBN 978-0-19-539784-0. doi: 10.1093/oxfordhb/9780195397840.013.0021

Moore, T., & Clayton, R. *The consequence of non-cooperation in the fight against phishing.* In *eCrime Researchers Summit, 2008,* pages 1-14. IEEE, October 2008. ISBN 978-1-4244-2969-1.
URL http://dx.doi.org/10.1109/ECRIME.2008.4696968

Moore, T., & Clayton, R. *Evaluating the wisdom of crowds in assessing phishing websites.* In *Financial cryptography and data security,* pages 16-30. Springer, Berlin, Heidelberg, 2008. ISBN 978-3-540-85229-2. doi: 10.1007/978-3-540-85230-8_2.

Morris, T., Pan, S., Lewis, J., Moorhead, J., Reaves, B., Younan, N., King, R., Freund, M., & Madani, V. *Cybersecurity testing of substation phasor measurement units and phasor data concentrators*. In *7th Annual ACM Cyber Security and Information Intelligence Research Workshop (CSIIRW),* pages 1-24. ACM, New York, NY, USA. ISBN 978-1-4503-0945-5.
URL http://dx.doi.org/10.1145/2179298.2179324

Moteff, J., & Parfomak, P. *Critical infrastructure and key assets: Definition and identification*. Online, October 2004. Last Accessed, 2013/06/21.
URL https://www.fas.org/sgp/crs/RL32631.pdf

Muallem, A., Shetty, S., & Hargrove, S. *Visualizing geolocation of spam email*. In *Computing, Communications and IT Applications Conference (ComComAp), 2013,* pages 63-68. IEEE. ISBN 978-1-4673-6043-2.
URL http://dx.doi.org/10.1109/ComComAp.2013.6533610

Naidoo, G., Singh, S., & Levine, N. *An overview of internet developments and their impact on E-government in south Africa.* In **Ajeeli, A., Thyab, A.,** editors, *Handbook of Research on E-Services in the Public Sector: E-Government Strategies and Advancements: E-Government Strategies and Advancements*, pages 63-77. Idea Group Inc, 2010. ISBN 1615207902.

National Institute of Standards and Technology (NIST), & United States of America. *Framework for improving critical infrastructure cybersecurity*. Online, February 2014. Last Accessed, 2014/04/16.
URL http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Organisation for Economic Co-operation and Development (OECD). *Cybersecurity policy making at a turning point* Online, November 2012. Last Accessed, 2013/09/22. doi:10.1787/5k8zq92vdgtl-en.
URL http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

O'Grady, M. J., Murdoch, O., Kroon, B., Lillis, D., Carr, D., Collier, R. W., & O'Hare, G. M. *Pervasive sensing: Addressing the heterogeneity problem*. J*ournal of Physics: Conference Series,* 450(1):012044, 2013. ISSN 1742-6596.
URL http://stacks.iop.org/1742-6596/450/i=1/a=012044

O'Harrow Jr, R. *Cyber search engine Shodan exposes industrial control systems to new risks*. Online, June 2012. Last Accessed, 2013/05/11.
URL http://www.cfr.org/cybersecurity/washpost-cyber-search-engine-shodan-exposes-industrial-control-systems-new-risks/p28431

Ophardt, J. A. *Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield*. *Duke Law & Tech Review* 2010(3):1-27, 2010. ISSN 2328-9600.
URL http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1198&context=dltr

Otis, J. R. *Evaluation of cyber sensors for enhancing situational awareness in the ICS environment.* Master's thesis, Department of Science in Computer Science, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA, June 2013.
URL http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA590483

Pal, R., Golubchik, L., Psounis, K., & Hui, P. *Will cyber-insurance improve network security: A market analysis*. In *INFOCOM, 2014 Proceedings,* pages 235-243, May 2014. IEEE. INSPEC 14430547.
URL http://dx.doi.org/10.1109/INFOCOM.2014.6847944

Pallaris, C. *Open source intelligence: A strategic enabler of national security*. *Center for Security Studies Analyses in Security Policy* 3(32):1-3, April 2008. ISSN 1863-0421.

Papadimitriou, P., & Garcia-Molina, H. *Data leakage detection. Knowledge and Data Engineering, IEEE Transactions On,* 23(1):51-63, Jan 2011. IEEE. ISSN: 1041-4347.
URL http://dx.doi.org/10.1109/TKDE.2010.100

Patnayakuni, R., & Patnayakuni, N. *Information security in value chains: A governance perspective*. In *Proceedings of the Twentieth Americas Conference on Information Systems, AMCIS 2014.* Pages 1-15, 2014. University of Georgia. ISBN 978-0-692-25320-5.

Permann, M. R., & Rohde, K. *Cyber assessment methods for SCADA security*. In *15th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference Proceedings,* pages –, 2005. ISBN 978-1556179495.

Piquero, N. L., Cohen, M. A., & Piquero, A. R. *How much is the public willing to pay to be protected from identity theft? Justice Quarterly,* 28(3):437-459, 2011. Routeledge. ISSN 0741-8825 doi: 10.1080/07418825.2010.511245.

Plohmann, D., Gerhards-Padilla, E., & Leder, F. *Botnets: Detection, measurement, disinfection & defence. European Network and Information Security Agency (ENISA).* Online, March 2011. Last Accessed: 2013/01/20.
URL https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/botnets-measurement-detection-disinfection-and-defence/at_download/fullReport

Poese, I., Uhlig, S., Kaafar, M. A., Donnet, B., & Gueye, B. *IP geolocation databases: Unreliable? ACM SIGCOMM Computer Communication Review,* 41(2):53-56. ACM, New York, NY, USA, 2011. ISSN 0146-4833.
URL http://dx.doi.org/10.1145/1971162.1971171

Polcák, L., Jirásek, J., & Matousek, P. *Comment on" remote physical device fingerprinting". IEEE Transactions on Dependable and Secure Computing,* pages 11(5):494-496, Sept 2014. IEEE Computer Society. ISSN 1545-5971.
URL http://doi.ieeecomputersociety.org/10.1109/TDSC.2013.26

Ponemon Institute. *2013 cost of data breach study: Global analysis.* Online, 2013. Last Accessed, 2014/07/05.
URL https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

Prieto, V. M., Alvarez, M., López-García, R., & Cacheda, F. *Analysing the effectiveness of crawlers on the client-side hidden web*. In **Rodriguez, J. M., Perez, J. B., Golinska, P., Giroux, S., Corchuelo, R., editors,** *Trends in practical applications of agents and multiagent systems, Proceedings of the 10th International Conference on Practical Applications of Agents and Multi-Agent Systems,* pages 141-148. Springer, Berlin, Heidelberg. ISBN 978-3-642-28794-7. doi: 10.1007/978-3-642-28795-4_17

PWC. *Why you should adopt the NIST cybersecurity framework.* Online, 2014. Last Accessed, 2014/09/22.
URL http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

PwC UK. *UK cyber security standards.* Online, 2013. Last Accessed, 2014/10/18.
URL https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/261681/bis-13-1294-uk-cyber-security-standards-research-report.pdf

Radvanosky, R. *Project SHINE.* Online, 2014. Last Accessed, 2014/10/21.
URL http://www.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014

Rao, J. M., & Reiley, D. H. *The economics of spam. The Journal of Economic Perspectives,* 26(3):87-110, 2012. American Economic Association. ISSN 0895-3309.
URL http://www.jstor.org/stable/41581133

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. *Anonymous connections and onion routing. Selected Areas in Communications, IEEE Journal On,* 16(4):482-494, 1998. IEEE. ISNN 0733-8716.
URL http://dx.doi.org/10.1109/49.668972

Ren, P., Kristoff, J., & Gooch, B. *Visualizing DNS traffic.* In *Proceedings of the 3rd International Workshop on Visualization for Computer Security,* pages 23-30, 2006. ISBN 1-59593-549-5.
URL http://dx.doi.org/10.1145/1179576.1179582

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. *Identifying, understanding, and analyzing critical infrastructure interdependencies. Control Systems, IEEE,* 21(6):11-25, 2001. IEEE. ISSN 1066-033X.
URL http://dx.doi.org/10.1109/37.969131

Ring, T. *Threat intelligence: Why people don't share. Computer Fraud & Security,* 2014(3):5-9, March 2014. Science Direct. ISSN 1361-3723.
URL http://dx.doi.org/10.1016/S1361-3723(14)70469-5

Rogova, G. L., & Bosse, E. *Information quality in information fusion*. In *Information Fusion 13th Conference On (FUSION) 2010,* pages 1-8, July 2010. IEEE. ISBN 978-0-9824438-1-1.
URL http://dx.doi.org/10.1109/ICIF.2010.5711857

Rohret, D., & Kraft, M. *Catch me if you can: Cyber anonymity*. In **Armistead, L.,** editor, *Proceedings of the 6th International Conference on Information Warfare and Security,* pages 213-219, 2011. Academic Conferences Limited. ISBN 1906638926.

Romanosky, S., Telang, R., & Acquisti, A. *Do data breach disclosure laws reduce identity theft? Journal of Policy Analysis and Management,* 30(2):256-286, 2011. Whiley Publishers. ISSN 1520-6688. doi: 10.1002/pam.20567.

Ruefle, R. M., & Murray, M. *CSIRT requirements for situational awareness*. Report, Carnegies Mellon Software Engineering Institutes, Fifth Avenue, Pittsburg, PA, USA, Jan 2014.
URL http://www.dtic.mil/get-tr-doc/pdf?AD=ADA596848

Sanger, D. E. *Obama Order Sped Up Wave of Cyberattacks Against Iran.* Online, June 2012. Last Accessed, 2013/04/23.
URL http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

SANS. *Security predictions 2012 & 2013 - the emerging security threat.* Online, 2011. Last Accessed, 2014/03/31.
URL http://www.sans.edu/research/security-laboratory/article/security-predict2011

Santorelli, S. *The global open resolver picture*. *Security Acts,* 2010(3):29-31, May 2010. Díaz & Hilterscheid Unternehmensberatung GmbH. ISSN 1869-4977.
URL http://www.securityacts.com/securityacts03.pdf

Scholz, R. W., & Tietje, O. *Embedded case study methods*. SAGE Publications, Inc, Thousand Oaks, USA, October 2013, pages 9-15. ISBN 9780761919452.

Schreiber-Ehle, S., & Koch, W. *The JDL model of data fusion applied to cyber-defence—A review paper*. In *Sensor Data Fusion: Trends, Solutions, Applications (SDF), 2012 Workshop On,* pages 116-119, 2012. ISBN 978-1-4673-3010-7. URL http://dx.doi.org/10.1109/SDF.2012.6327919

Shabtai, A., Elovici, Y., & Rokach, L. *A taxonomy of data leakage prevention solutions*. In *A survey of data leakage detection and prevention solutions,* pages 11-15, 2012. Springer US. ISBN 978-1-4614-2052-1. doi:10.1007/978-1-4614-2053-8_3.

Shanteau, J., & Stewart, T. R. *Why study expert decision making? Some historical perspectives and comments*. *Organizational Behavior and Human Decision Processes, 53*(2):95-106, November 1991. Science Direct. ISSN 0749-5978. URL http://dx.doi.org/10.1016/0749-5978(92)90057-E

Shay, L. A., Conti, G., & Hartzog, W. *Beyond sunglasses and spray paint: A taxonomy of surveillance countermeasures*. In *Technology and Society (ISTAS), 2013 IEEE International Symposium On,* pages 191-200, June 2013. ISBN 978-1-4799-1242-1. URL http://dx.doi.org/10.1109/ISTAS.2013.6613118

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. *Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions*. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* pages 373-382. ISBN 978-1-60558-929-9. URL http://dx.doi.org/10.1145/1753326.1753383

Shneiderman, B. *The eyes have it: A task by data type taxonomy for information visualizations*. In *Visual Languages, 1996 Proceedings., IEEE Symposium On,* pages 336-343, 1996. IEEE. ISBN 0-8186-7508-X. URL http://dx.doi.org/10.1109/VL.1996.545307

Shteiman, B. *Why CMS platforms are breeding security vulnerabilities*. *Network Security, 2014*(1):7-9, January 2014. Elsevier Science Publishers, Amsterdam, The Netherlands. ISSN 1816-3548. URL http://dx.doi.org/10.1016/S1353-4858(14)70006-6

Sisson, G. *DNS Survey: October 2010.* Online, November 2010. Last Accessed, 2014/02/19.
URL http://dns.measurement-factory.com/surveys/201010/dns_survey_2010.pdf

Smets, P. (1993). *Belief functions: The disjunctive rule of combination and the generalized bayesian theorem*. *International Journal of Approximate Reasoning,* 9(1):1-35, August 1993. Science Direct. ISSN 0888-613X.
URL http://dx.doi.org/10.1016/0888-613X(93)90005-X

Smets, P., & Kennes, R. *The transferable belief model*. *Artificial Intelligence,* 66(2):191-234, April 1994. Science Direct. ISSN 0004-3702.
URL http://dx.doi.org/10.1016/0004-3702(94)90026-4

Sokolova, M., El Emam, K., Arbuckle, L., Neri, E., Rose, S., & Jonker, E. *P2P watch: Personal health information detection in peer-to-peer file-sharing networks*. *Journal of Medical Internet Research,* 14(4):e95, July 2012. ISSN 1438-8871. doi: 10.2196/jmir.1898

Spring, J. M. *Modeling malicious domain name take-down dynamics: Why eCrime pays*. In *The eCrime Researchers Summit (eCRS),* September 2013:1-9, 2013. IEEE.
URL http://dx.doi.org/10.1109/eCRS.2013.6805779

Stalmans, E., & Irwin, B. *A framework for DNS based detection and mitigation of malware infections on a network*. In *Information Security South Africa (ISSA),* pages 1-8, August 2011. IEEE. ISBN 978-1-4577-1481-8.
URL http://dx.doi.org/10.1109/ISSA.2011.6027531

Steinberg, A. N., Bowman, C. L., & White, F. E. *Revisions to the JDL data fusion model*. In *AeroSense'99,* pages 430-441. doi:10.1117/12.341367.

Swart, I. *Practical application of open source frameworks to achieve anti-virus avoidance*. In **Filiol, E., Erra, R.,** editors, *Proceedings of the 11th European conference on Information Warfare and Security*, pages 265-275. Academic Conferences Limited, London, UK, 2012. ISSN 2048-9870. ISBN 978-1-908272-55-3.

Swart, I., Grobler, M. M., & Irwin, B. *Visualization of a data leak*. In *Information Security for South Africa, 2013,* pages 1-8, Aug 2013. IEEE. doi:10.1109/ISSA.2013.6641046.

Szewczyk, P. *Usability and security support offered through ADSL router user manuals*. In *Proceedings of the 11th Australian Information Security Management Conference*, pages –, December 2013. Edith Cowan University, Perth, Western Australia. URL http://ro.ecu.edu.au/ism/160/

Tadda, G. P., & Salerno, J. S. *Overview of cyber situation awareness*. In **Jajodia, S., Liu, P., Swarup, V., Wang, C.** editors, *Cyber situational awareness,* 46:15-35, Springer US. 2010. ISSN 1568-2633. ISBN 978-1-4419-0139-2. doi:10.1007/978-1-4419-0140-8_2.

Taylor, J., Devlin, J., & Curran, K. *Bringing location to ip addresses with ip geolocation*. *Journal of Emerging Technologies in Web Intelligence,* 4(3):273-277, August 2012. Academy Publishers. ISSN 1798-0461. doi:10.4304/jetwi.4.3.273-277.

Timonen, J., Lääperi, L., Rummukainen, L., Puuska, S., & Vankka, J. *Situational awareness and information collection from critical infrastructure*. In *2014 6th International Conference on Cyber Conflict CYCON 2014,* pages 157-173, June 2014. IEEE. ISBN 978-9949-9544-0-7. URL http://dx.doi.org/10.1109/CYCON.2014.6916401

van Rooyen, C. *An empirical study of open source web application software deployment and its associated risks in the ZA namespace.* Master's thesis, University of South Africa, Pretoria, February 2014. URL https://www.academia.edu/7900760/An_empirical_study_of_open_source_web_application_software_deployment_and_its_associated_risks_in_the_ZA_namespace

Vanderbeken, E. *TCP/32764 backdoor.* Online, April 2013. Last Accessed, 2014/10/11. URL https://github.com/elvanderb/TCP-32764/blob/master/backdoor_description.pptx

Verizon. *The 2013 data breach Investigations Report*. Online, 2013. Last Accessed, 2014/12/24. URL http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

von Solms, R., & van Niekerk, J. *From information security to cyber security*. *Computers & Security,* 38:97-102, October 2013. Science Direct. ISSN 0167-4048. URL http://dx.doi.org/10.1016/j.cose.2013.04.004

Vratonjic, N., Huguenin, K., Bindschaedler, V., & Hubaux, J. *A location-privacy threat stemming from the use of shared public IP addresses*. *IEEE Transactions on Mobile Computing,* 13(11):2445-2457, November 2014. IEEE. ISSN 1536-1233. URL http://dx.doi.org/10.1109/TMC.2014.2309953

Waltz, E. *Knowledge management in the intelligence enterprise*. Artech House Publishers, Boston, USA, April 2003, 376 pages. ISBN 1-58053-494-5.

Waltz, E., & Llinas, J. *Multisensor data fusion*. Artech House Publishers, Boston, USA, Augustus 1990, 464 pages. ISBN 0890062773.

Wang, G., Zhang, C., Qiu, X., & Zeng, Z. *Modelling a tractable and annotated ISP's router-level topology based on statistical data and geolocation mapping*. In **Gilbert. K., Botti, V., Reig-Bolaño, R.,** editors, *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference On,* pages 31-35. ISBN 978-1-61284-485-5. URL http://dx.doi.org/10.1109/ICCSN.2011.6013539

Wang, Y., Burgener, D., Flores, M., Kuzmanovic, A., & Huang, C. *Towards street-level client-independent IP geolocation*. In *NSDI'11. In Proceedings of the 8th USENIX Conference on Networked Systems Design and Implementation,* pages 365-379, 2011. USENIX Association, Berkely, CA, USA.

Warren, M., & Leitch, S. *Australian National Critical Infrastructure Protection: A Case Study*. In **Ottis, R.,** editor, *Proceedings of the 10th European Conference on Information Warfare and Security,* pages 275-280. Academic Conferences Limited, London, UK, 2011. ISBN 1908272066.

Weimann, G. *Www. terror. net: How modern terrorism uses the internet*. Diane Publishing Co, Rear Collingdale, US, 2004, 11 pages. ISBN 9781437904161.

White, F. *Data Fusion Lexicon: Data Fusion Subpanel of the Joint Directors of Laboratories Technical Panel for C3.* Online, October 1991. Last Accessed, 2014/11/18. URL http://www.dtic.mil/dtic/tr/fulltext/u2/a529661.pdf

Wilkinson, L., & Friendly, M. *The history of the cluster heat map. The American Statistician,* 63(2):179-184. Thompson Reuters. ISSN 0003-1305. doi:10.1198/tas.2009.0033.

Williams, G. *Cost effective assessment of the infrastructure security posture*. In *System Safety, Incorporating the Cyber Security Conference 2012, 7th IET International Conference On,* pages 1-6. IET, October 2012. URL http://dx.doi.org/10.1049/cp.2012.1503

Williams, P. *Distinguishing internet-facing ICS devices using PLC programming information.* Master's thesis, Department of the Air Force University, Wright-Patterson Air Force Base, Ohio, USA, June 2014. URL https://www.hsdl.org/?view&did=757013

Xiang, X., Wang, X., & Zhou, Z. *Self-adaptive on-demand geographic routing for mobile ad hoc networks*. *IEEE Transactions On Mobile Computing,* 11(9):1572-1586, September 2012. IEEE. ISSN 1536-1233. URL http://dx.doi.org/10.1109/TMC.2011.177

Yang, S. J., Stotz, A., Holsopple, J., Sudit, M., & Kuhl, M. *High level information fusion for tracking and projection of multistage cyber attacks*. *Information Fusion,* 10(1):107-121. Elsevier Science Publishers, Amsterdam, The Netherlands, January 2009. ISSN 1566-2535. URL http://dx.doi.org/10.1016/j.inffus.2007.06.002

Zhang, J., Yang, C., Xu, Z., & Gu, G. *Poisonamplifier: A guided approach of discovering compromised websites through reversing search poisoning attacks*. In **Balzarotti, D., Stolfo, S. J., Cova, M.,** editors, *Research in attacks, intrusions, and defences, 15th International Symposium, RAID 212,* pages 230-253. Springer, Berlin, Heidelberg, September 2012. ISBN 978-3-642-33337-8. doi: 10.1007/978-3-642-33338-5_12.

Zhura, M. *Cybercrime: It's serious, but exactly how serious? Communications of the ACM,* 56(3):18-20, 2013. ISSN 0001-0782. URL http://dl.acm.org/ft_gateway.cfm?id=2428563&type=html

Appendices

A

PhishTank Data

Table A-1 presents the raw data taken from a snapshot captured on 2014-06-24. The data contains all directly or indirectly phishing-related information for the .co.za domain in the given period. These entries are all either hosted in the South African .co.za domain, or .co.za host is referenced in the submit URL of a phish. At the very least all hosts listed should be investigated for possible hacking activity due to their involvement with potential phishing scams. The results of this data is detailed in Section 4.4.5 and indicates that while PhishTank is highly useful, the reliability of the data is questionable and should not be used without verification.

The columns from left to right indicate:

- Phishing URL – The URL that was used to host the phishing website.
- Target – Who the phisher impersonated according to PhishTank analysts.
- ID – The unique ID assigned by PhishTank to this specific reported incident.
- Available – Indicates if the page was still available at the time of the investigation.
    - The options are Yes, No, Corrected or Timeout.
        - Yes indicates it could be accessed at the time of evaluation.
        - No indicates that the page is not accessible anymore.
        - Corrected indicates that the phishing page has been removed and correct functionality has been restored.
        - A timeout value indicates that the DNS still resolves but that the server is not responding.
- Target Examined – Who the phisher impersonated, according to the researcher.
- Blocked – Even if the URL is still available, has it been blocked by the Firefox or Internet explorer browser.
    - The only options are Yes or No.

Table A-1: PhishTank data affecting the .co.za domain on 24/06/2014

Phishing URL	Target	ID	Available	Target Examined	Blocked
http://www.itcompliance.co.za/libraries/joomla/won.php	Santander UK	2546770	No	Santander	No
http://ncrdebtcounsellor.co.za/joomdocs/Alibaba-login.jsp.html	Other	2545790	No	Alibaba	No
http://www.ncrdebtcounsellor.co.za/joomdocs/Alibaba-login.jsp.html	Other	2545603	Yes	Alibaba	Yes
http://www.hashalom.co.za/us.mc1254.mail.Yahoo.htm	Other	2541841	Yes	Yahoo	Yes
http://www.mindint.co.za/novus/libraries/zauan/shortcodes/google_maps/googledot	Other	2541677	Yes	Google, Yahoo, AOL, Windows	No
http://www.mindint.co.za/novus/libraries/zauan/shortcodes/google_maps/googledot/	Other	2541398	No	Google, Yahoo, AOL, Windows	No
http://mugsforsale.co.za/2013gdocs	Other	2540793	No	Google docs	No
http://www.mindint.co.za/novus/libraries/zauan/shortcodes/google_maps/googledot/index.htm	Other	2540371	Yes	Google, Yahoo, AOL, Windows	No
http://www.mindint.co.za/novus/administrator/components/com_breezingforms/libraries/tcpdf/config/google_maps/googledot/index.htm	Other	2540360		Google, Yahoo, AOL, Windows	No
http://k3mremovals.co.za/plugins/editors/tinymce/jscripts/tiny_mce/plugins/fullpage/images/pulign/8f9ca053a1a6a33583f79ba212dd009b/	PayPal	2539768	No	PayPal	Yes
http://boegoebergecoroute.co.za/bt/index.htm	Other	2537857	No	BT	Yes
http://eastcoastshuttleservices.co.za/images/google.document.html	Other	2528546	Yes	Google, Yahoo, AOL, Windows	Yes

Phishing URL	Target	ID	Available	Target Examined	Blocked
http://happyball.ru/includes/domit/cm/8365ab77a866851f8cb8e632847a8a8d/lb.php?id=13698&default=f75744b9b40378836b6de07651f968b4,http://www.elka.sklep.pl/logs/oldoppfllfopp/32368eb65ffb06680aaa255fc32e06fc/,http://nadiadutoit.co.za/update/5938780f430d1c07ee859518ede6a797/,http://private-itm.com/test/secure-listings-redirect/products/ebaymotors/pages/SignIn.php?co_partnerId=2	eBay, Inc.	2524646	Yes	Credit and Mutual	No
http://midcityklerksdorp.co.za/	Other	2523055	Corrected	Google Docs	No
http://www.scottstours.co.za/%7Eresumema/pay/new2014/home/paypal.php	Other	2520032	Corrected	PayPal	Yes
http://www.scottstours.co.za/~resumema/pay/new2014/home/paypal.php	Other	2520031	Corrected	PayPal	Yes
http://kilburn.co.za/paypal.php	PayPal	2519907	Yes	PayPal	Yes
http://www.stockowners.co.za/~resumema/pay/new2014/home/paypal.php?action=billing_login=true	Other	2519719	Corrected	PayPal	No
http://www.stockownersbusinesspark.co.za/~resumema/pay/new2014/home/paypal.php?action=billing_login=true	Other	2519715	Corrected	PayPal	Yes
http://www.scottstours.co.za/~resumema/pay/new2014/home/paypal.php?action=billing_login=true	Other	2519611	Corrected	PayPal	No
http://happyball.ru/includes/domit/cm/8365ab77a866851f8cb8e632	Other	2512454	Yes	Credit and Mutual	No

Phishing URL	Target	ID	Available	Target Examined	Blocked
847a8a8d/lb.php?id=13698&default=f75744b9b40378836b6de07651f968b4,http://185.7.215.24/be0ecd5860d91895f7a04d6aaa568014/websc.php?cmd=login_submit,http://nadiadutoit.co.za/update/5938780f430d1c07ee859518ede6a797/,http://nicnieuwoudt.com/wp-includes/Text/start.php					
http://happyball.ru/includes/domit/cm/8365ab77a866851f8cb8e632847a8a8d/lb.php?id=13698&default=f75744b9b40378836b6de07651f968b4,http://nadiadutoit.co.za/update/5938780f430d1c07ee859518ede6a797/,http://support-teams.com/websc.php?id=07c0189ff23a3fec,http://g-team.org.ve/~acuamoda/js/a/359d6f8a0481cba111d135aa360ab279/sais.php?id=225488966665	Other	2512453	Yes	Credit and Mutual	No
http://www.maselwafamilyfunerals.co.za/.smileys/Yahoo/Yahoo.html	Other	2505227	Yes	Yahoo	Yes
http://maselwafamilyfunerals.co.za/.smileys/Yahoo/Yahoo.html	Other	2505042	Yes	Yahoo	Yes
http://paypal-europe.corporatecabs.co.za/?cmd=_home/	Other	2497285	No	PayPal	No
http://mugsforsale.co.za/2013gdocs/	Other	2493248	Yes	Google, Yahoo, AOL, Windows	No
http://dorrypets.co.za/formm.html	Other	2491939	No	Other	Yes

Phishing URL	Target	ID	Available	Target Examined	Blocked
http://www.lovemycar.co.za/images/smilies/won.php	Nationwide Building Society	2478985	No	Other	Yes
http://mugsforsale.co.za/2013gdocs/index.htm	Other	2474332	Yes	Google, Yahoo, AOL, Windows	No
http://diketconnection.co.za/googledocss/sss	Other	2473221	Yes	Google, Yahoo, AOL, Windows	Yes
http://diketconnection.co.za/googledocss/sss/	Other	2465863	Yes	Duplicate	Yes
http://www.worded.co.za/googledocss/s/indexpage.htm	AOL	2465480		Duplicate	
http://tailormadestaffing.co.za/g_doc/file_doc.php	Other	2465379	Yes	Google	Yes
http://diketconnection.co.za/googledocss/sss/index.htm	AOL	2465337		Duplicate	
http://www.hitfactoryrecords.co.za/aol.html	AOL	2465305	Yes	AOL	Yes
http://redvisionsa.co.za/pip/GoogleSecure.htm	Google	2460380	Yes	Google	Yes
http://googledocs.aecswimming.co.za/	Other	2452359	Yes	Google, Yahoo, AOL, Windows	Yes
http://lighthouseelectronics.co.za/media/media/images/doc/	Other	2449728	No	Google, Yahoo, AOL, Windows	Yes
http://timeoutmin.co.za/images/stories/Activ/PayPal/webscrcmd%3D_login-submit%26dispatch%3D5885d80a13c0db1ffc45dc241d84e9538c532da79baccf7c26f850d773643350/paypal/	Other	2407695	No	PayPal	No
http://scmotors.co.za/images/webmail.maxnet.co.nz/login.html	Other	2386405	Yes	MaxNet	Yes
http://www.verify-your-information-1qs5dc1qs6541q5sf1sq	Other	2384760	Timeout	Other	

Phishing URL	Target	ID	Available	Target Examined	Blocked
f1qs5.adullamconsulting.co.za/reactivation/473497faa4c30599401c42cd683c8a9f/?cmd=_home&dispatch=30e59744a0dd06a88b640e9835493e4530e59744a0dd06a88b640e9835493e45					
http://www.verify-your-information-1qs5dc1qs6541q5sf1sqf1qs5.adullamconsulting.co.za/reactivation/473497faa4c30599401c42cd683c8a9f/?cmd=_home&dispatch=15cea334ce1f869fdd3317d788b6904c15cea334ce1f869fdd3317d788b6904c	Other	2384759		Other	
http://www.verify-your-information-1qs5dc1qs6541q5sf1sqf1qs5.adullamconsulting.co.za/reactivation/473497faa4c30599401c42cd683c8a9f/?cmd=_home&dispatch=94a245f1e21001fc1d13eb40c1be71f094a245f1e21001fc1d13eb40c1be71f0	Other	2384758		Other	
http://www.verify-your-information-1qs5dc1qs6541q5sf1sqf1qs5.adullamconsulting.co.za/reactivation/	PayPal	2382139		PayPal	
http://fabbri.co.za/doc/file.index.htm	Other	2359182	Yes	Google, Yahoo, AOL, Windows	Yes
http://teambuildingworkshops.co.za/capitec_eft_notice.php	Other	2329033	No	Capitec	No
http://analogstereo.com/images/turntable/FNB.CO.ZA/fnb.co.za.html	Other	2320271	Yes	FNB	No
http://showofhands.co.	Other	2296572	Corrected	Other	No

Phishing URL	Target	ID	Available	Target Examined	Blocked
za/includes/alinew/inq.html					
http://www.paypal.com.cgi-bin.webscr.accountflowsession.5885d80a13c0db1263663dssf22f3faeea2d883d446d7sfg9231u08k30646.8df79z8et12332z5367dsf4634dsse346324dry575457ft467548.bluewave.co.za/	Other	2271918	No	Paypal	No
http://switchphone.co.za/libraries/index.html	Other	2233215	Yes	Yahoo	No
http://mediaghat.com/ajaxjs/admin/modules/FNB/www1.fnb.co.za/index.html	Other	951179	Yes	FNB	No

B

The MITRE measurable category list

While Figure 3-2 illustrates the core components that can be used to calculate the attack surface of a security system, it lacks increased detail regarding the factors that contribute to overall security. For a better understanding of all the areas that need to be evaluated, the MITRE corporation's categorical breakdown serves as a solid base. Instead of attempting to provide metrics that can be used in an organization, the categories detail all possible areas that have to be considered when assessing security (MITRE, 2013). By extending the categories and incorporating standards that can be used to uniquely describe each category, this attempt aims to standardize the environment instead of just applying some form of metric. Their work provides a comprehensive guide to the areas that are typically affected when cyber security needs to be managed. In the event that a nation has progressed far enough with national cyber security implementation based on the simplified attack surface previously presented, the extended categories could further increase attention to detail. A summary regarding all the areas follows.

A.1 SOFTWARE ASSURANCE

Software assurance can be defined as the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the correct manner.

A.2 APPLICATION SECURITY

The degree of trust in the application's ability to perform as designed despite unplanned user actions or deliberate attacks. Frameworks and recommendations such as OWASP Top 10, CWE/SANS Top 25, Common Weakness risk Analysis Framework (CWRAF) or Common Weakness Scoring Systems (CWSS) can be utilized to assess the confidence level in the software.

A.3 ASSET MANAGEMENT

Without sufficient inventory implementations, it will not be possible to examine risk against know vulnerabilities. Various schemas exist to ensure information sharing compatibility between systems, such as Open Vulnerability and Assessment Language (OVAL) or Asset Summary Reporting (ASR).

A.4 SUPPLY CHAIN RISK MANAGEMENT

ICT equipment is typically sourced from a variety of vendors and in general most vendors' products work well with products from other vendors. However, the vendor's security posture can affect the organization using the produced product by compromising confidentiality, integrity and patch cycles. Supply Chain Risk Management (SCRM) can use formats such as Observable eXpression (CybOX) to describe all aspects of the supply chain equipment.

A.5 CYBER INTELLIGENCE THREAT ANALYSIS

Information relating to attacks against the organization such as phishing can be shared to increase awareness among different employees or companies. Various standard implementations such as Structured Threat Information Expression (STIX) or Cyber Observable Expression (CybOX) can be used. The implementations make use of standards such as Common Vulnerability and Exposure (CVE), Common Weakness Enumeration (CWE).

A.6 CYBER THREAT INFORMATION SHARING

By sharing information between organizations, understanding of the technical methods and the methods of attack can be achieved. Sharing Tactics, Techniques and Procedures (TTPs) allows organizations to force attackers to work harder for every target. The information can be shared via STIX.

A.7 VULNERABILITY MANAGEMENT

This pertains to the level of disclosed security vulnerabilities available on the organizational infrastructure, e.g. CVEs. Should the organization also create software, it also applies to the ability to implement and distribute patches for the created software.

A.8 PATCH MANAGEMENT

The ability of the organization to effectively apply patches to infrastructure once a vulnerability has been disclosed and a fix made available.

A.9 CONFIGURATION MANAGEMENT

While different users typically require different ICT configurations, making use of a standard is still essential. Checking the adherence to a standard can be achieved via protocols such as Common Configuration Enumeration (CCE).

A.10 MALWARE PROTECTION

Attackers typically make use of malware to gain access to network infrastructure. While no current implementation of anti-virus is perfect, log files will aid in the creation of Open Indicators of Compromise (OpenIOC) reports.

A.11 INTRUSION DETECTION

While it is extremely hard to secure all avenues of entry to the corporate infrastructure, intrusion detection often assists to prevent intruders even when vulnerabilities exist. This is also useful for information sharing between organizations.

A.12 SYSTEM ASSESSMENT

By assessing a system for known vulnerabilities and indicators of compromise, the integrity of the system can be validated.

A.13 INCIDENT COORDINATION

In extreme events attacks could affect numerous parties or require information sharing with third parties. The ability to share information in such a manner that everyone understands is of critical importance.

A.14 Enterprise reporting

Sharing of metrics is one of the most basic requirements often overlooked in information security. The ability to communicate the security status quo to business is vitally important.

A.15 Remediation

Once a breach is detected, business is typically suspended until the systems can be restored to a trustworthy state. The process to achieve that relies on the ability to pinpoint the problem, implementing a action plan for cleanup and restoring to previous state from backups.

C

Software used and electronic resources

This study used a variety of both open source and free for use applications and data sources. The comprehensive list of resources used as well as the official description is included in Table C-1.

Table C-1: Software used in the construction of the experimental system

Id	Description/Release Notes
Antlr	ANother Tool for Language Recognition, is a language tool that provides a framework for constructing recognizers, interpreters, compilers, and translators from grammatical descriptions containing actions in a variety of target languages.
chosen	Chosen is a JavaScript plugin that makes long, unwieldy select boxes much more user-friendly. It is currently available in both jQuery and Prototype flavors.
chosen.jquery	Chosen is a JavaScript plugin that makes long, unwieldy select boxes much more user-friendly. It is currently available in both jQuery and Prototype flavors.
DocaLabs.Http.Client	Strong typed HTTP client. The main goal of the library is to minimize plumbing code to bare minimum.
DocaLabs.Http.Client.with.NewtonSoft.Json.Serializer	Strong typed HTTP client with provider using. The main goal of the library is to minimize plumbing code to bare minimum.
DocumentFormat.OpenXml	Microsoft OpenXML SDK 2.5
DotNetZip	A fork of the DotNetZip project without signing with a solution that compiles cleanly. This project aims to follow semver to avoid versioning conflicts. DotNetZip is a FAST, FREE class library and toolset for manipulating zip files. Use VB, C# or any .NET language to easily create, extract, or update zip files.
EntityFramework	Entity Framework is Microsoft's recommended data access technology for new applications.
ExcelDataReader	Lightweight and fast library written in C# for reading Microsoft Excel files ('97-2007).
IronPython	IronPython is an open-source implementation of the Python programming language which is tightly integrated with the .NET Framework. IronPython can use the .NET Framework and Python libraries, and other .NET languages can use Python code just as easily.
IronPython.StdLib	The Python Standard Library, for use with IronPython.
iTextSharp	iTextSharp is a port of the iText open source java library for PDF generation written entirely in C# for the .NET platform.
jQuery	jQuery is a new kind of JavaScript Library. jQuery is a fast and concise JavaScript Library that simplifies HTML document traversing, event handling, animating, and Ajax interactions for rapid web development. jQuery is designed to change the way that you write JavaScript. NOTE: This package is maintained on behalf of the library owners by the NuGet Community Packages

	project at http://nugetpackages.codeplex.com/
jquery.datatables	DataTables is a plug-in for the jQuery Javascript library. It is a highly flexible tool, based upon the foundations of progressive enhancement, which will add advanced interaction controls to any HTML table.
jQuery.UI.Combined	jQuery UI is an open source library of interface components — interactions, full-featured widgets, and animation effects — based on the stellar jQuery javascript library . Each component is built according to jQuery's event-driven architecture (find something, manipulate it) and is themeable, making it easy for developers of any skill level to integrate and extend into their own code. NOTE: This package is maintained on behalf of the library owners by the NuGet Community Packages project at http://nugetpackages.codeplex.com
jQuery.Validation	This jQuery plugin makes simple clientside form validation trivial, while offering lots of option for customization. That makes a good choice if you're building something new from scratch, but also when you're trying to integrate it into an existing application with lots of existing markup. The plugin comes bundled with a useful set of validation methods, including URL and email validation, while providing an API to write your own methods. All bundled methods come with default error messages in english and translations into 32 languages.
	NOTE: This package is maintained on behalf of the library owners by the NuGet Community Packages project at http://nugetpackages.codeplex.com
knockoutjs	A JavaScript MVVM library to help you create rich, dynamic user interfaces with clean maintainable code
leaflet	Leaflet is a modern open-source JavaScript library for mobile-friendly interactive maps.
Microsoft.AspNet.Mvc	This package contains the runtime assemblies for ASP.NET MVC. ASP.NET MVC gives you a powerful, patterns-based way to build dynamic websites that enables a clean separation of concerns and that gives you full control over markup.
Microsoft.AspNet.Providers.Core	ASP.NET Universal Providers add provider support in ASP.NET 4 for all editions of SQL Server 2005 and later and to SQL Azure. If you use these providers to develop your application, the application will be ready for cloud environments like Azure. Other than supporting additional storage options, the providers work like the existing SQL-based providers, so that you can easily switch an application to use cloud storage via SQL Azure.
Microsoft.AspNet.Providers.LocalDB	ASP.NET Universal Providers add provider support in ASP.NET 4 for all editions of SQL Server 2005 and later and to SQL Azure. If you use these providers to develop your application, the application will be ready for cloud environments like Azure. Other than supporting additional storage options, the providers work like the existing SQL-based providers, so that you can easily switch an application to use cloud storage via SQL Azure.
Microsoft.AspNet.Razor	This package contains the runtime assemblies for ASP.NET Web Pages. ASP.NET Web Pages and the new Razor syntax provide a fast, terse, clean and lightweight way to combine server code with HTML to create dynamic web content.
Microsoft.AspNet.Web.Optimization	ASP.NET Optimization introduces a way to bundle and optimize CSS and JavaScript files.
Microsoft.AspNet.WebApi.Client	This package adds support for formatting and content negotiation to System.Net.Http. It includes support for JSON, XML, and

	form URL encoded data
Microsoft.AspNet.WebApi.Core	This package contains the core runtime assemblies for ASP.NET Web API. This package is used by hosts of the ASP.NET Web API runtime. To host a Web API in IIS use the Microsoft.AspNet.WebApi.WebHost package. To host a Web API in your own process use the Microsoft.AspNet.WebApi.SelfHost package.
Microsoft.AspNet.WebApi.OData	This package contains everything you need to create OData endpoints using ASP.NET Web API and to support OData query syntax for your web APIs.
Microsoft.AspNet.WebApi.WebHost	This package contains everything you need to host ASP.NET Web API on IIS. ASP.NET Web API is a framework that makes it easy to build HTTP services that reach a broad range of clients, including browsers and mobile devices. ASP.NET Web API is an ideal platform for building RESTful applications on the .NET Framework.
Microsoft.AspNet.WebPages	This package contains core runtime assemblies shared between ASP.NET MVC and ASP.NET Web Pages. This packages enables projects targeting down-level platforms to use some of the types added in later versions including: CallerMemberNameAttribute CallerLineNumberAttribute CallerFilePathAttribute IStructuralComparable IStructuralEquatable Task InvalidDataException These types are "unified" to their later version equivalent. For example, when running on .NET Framework 4.5, IProgress<T> from this package will be seen by the runtime as the same type as the one already available in the platform. Supported Platforms: - .NET Framework 4 (with KB2468871) - Windows Phone 7.5 - Silverlight 4 and 5
Microsoft.Bcl	This package is only required for projects targeting .NET Framework 4.5, NET for Windows Store apps or Windows Phone 8 when consuming a library that uses this package.
Microsoft.Bcl.Build	This package provides build infrastructure components so that projects referencing specific Microsoft packages can successfully build. Do not directly reference this packages unless you receive a build warning that instructs you to add a reference.
Microsoft.Data.Edm	Classes to represent, construct, parse, serialize and validate entity data models. Targets .NET 4.0, Silverlight 4.0, or .NET Portable Lib with support for .NET 4.0, SL 4.0, Win Phone 7, and Win 8. Localized for CHS, CHT, DEU, ESN, FRA, ITA, JPN, KOR and RUS.
Microsoft.Data.OData	Classes to serialize, deserialize and validate OData payloads. Enables construction of OData producers and consumers. Targets .NET 4.0, Silverlight 4.0 or .NET Portable Lib with support for .NET 4.0, SL 4.0, Win Phone 7, and Win 8. Localized for CHS, CHT, DEU, ESN, FRA, ITA, JPN, KOR and RUS.
Microsoft.jQuery.Unobtrusive.Ajax	jQuery plugin that unobtrusively sets up jQuery Ajax.

Microsoft.jQuery.Unobtrusive.Validation	jQuery plugin that unobtrusively sets up jQuery.Validation.
Microsoft.Net.Http	This package includes HttpClient for sending requests over HTTP, as well as HttpRequestMessage and HttpResponseMessage for processing HTTP messages. This package is not supported in Visual Studio 2010, and is only required for projects targeting .NET Framework 4.5 or .NET for Windows Store apps when consuming a library that uses this package. Supported Platforms: - .NET Framework 4 - .NET for Windows Store apps - Windows Phone 7.5 and 8 - Silverlight 4 and 5
Microsoft.Web.Infrastructure	This package contains the Microsoft.Web.Infrastructure assembly that lets you dynamically register HTTP modules at run time.
Modernizr	Modernizr adds classes to the <html> element which allow you to target specific browser functionality in your stylesheet. You don't actually need to write any Javascript to use it. Modernizr is a small and simple JavaScript library that helps you take advantage of emerging web technologies (CSS3, HTML5) while still maintaining a fine level of control over older browsers that may not yet support these new technologies. NOTE: This package is maintained on behalf of the library owners by the NuGet Community Packages project at http://nugetpackages.codeplex.com/
Newtonsoft.Json	Json.NET is a popular high-performance JSON framework for .NET
Newtonsoft.Json	Json.NET is a popular high-performance JSON framework for .NET
RestSharp	Simple REST and HTTP API Client
SharpZipLib	#ziplib (SharpZipLib, formerly NZipLib) is a Zip, GZip, Tar and BZip2 library written entirely in C# for the .NET platform. It is implemented as an assembly (installable in the GAC), and thus can easily be incorporated into other projects (in any .NET language).
System.Spatial	Contains classes and methods that facilitate geography and geometry spatial operations. Targets .NET 4.0, Silverlight 4.0 or .NET Portable Lib with support for .NET 4.0, SL 4.0, Win Phone 7, and Win 8. Localized for CHS, CHT, DEU, ESN, FRA, ITA, JPN, KOR and RUS.
TweetSharp	TweetSharp v2 is a fast, clean wrapper around the Twitter API. It uses T4 templates to make adding new endpoints easy.
WebGrease	Web Grease is a suite of tools for optimizing javascript, css files and images.

The DVD accompanying this documents contains introductory videos of the experimental system constructed during the course of this study. Other resources such as the generated leet speak dictionaries previously discussed in Section 4.5.4 has also been made available.

D

Previous publications

I. Swart, B. Irwin, M.M Grobler:"*Multi sensor national cyber security data fusion.*" Accepted and to be presented on the 24th March 2015 at the 10th International Conference on Cyber Warfare and Security ICCWS-2015.

Abstract

A proliferation of cyber security strategies have recently been published around the world with as many as thirty five strategies documented since 2009. These published strategies indicate the growing need to obtain a clear view of a country's information security posture and to improve on it. The potential attack surface of a nation is extremely large however and no single source of cyber security data provides all the required information to accurately describe the cyber security readiness of a nation. There are however a variety of specialized data sources that are rich enough in relevant cyber security information to assess the state of a nation in at least key areas such as botnets, spam servers and incorrectly configured hosts present in a country. While informative both from an offensive and defensive point of view, the data sources range in a variety of factors such as accuracy, completeness, representation, cost and data availability. These factors add complexity when attempting to present a clear view of the combined intelligence of the data. By applying data fusion the potential exists the potential exists to provide a comprehensive and representative view of all data sources fused together, regardless of their complexity. This method is not often used in cyber defense systems, since cyber sensor data is typically hard to classify in traditional data fusion techniques due to the diversity and ambiguity present in the sources. This research will examine a variety of currently available Internet data sources and apply it to an adapted Joint Directors of Laboratories (JDL) data fusion model. The model has been adapted to suit national level cyber sensor data fusion with the aim to formally define and reduce data ambiguity and enhance fusion capability in a real world system. The data examined will then be applied to a case study that will show the results of applying available open source security information against the model to relate to the current South African cyber landscape.

Swart, I., Irwin, B. and Grobler, M: "*On the viability of pro-active automated PII breach detection: A South African case study*." Proceedings of the Southern African Institute for Computer Scientist and Information Technologists Annual Conference (SAICSIT) 2014 Empowered by Technology. ACM, 2014.

Abstract

Various reasons exist why certain types of information is deemed personal both by legislation and society. While crimes such as identity theft and impersonation have always been in existence, the rise of the internet and social media has exacerbated the problem. South Africa has recently joined the growing ranks of countries passing legislation to ensure the privacy of certain types of data. As is the case with most implemented security enforcement systems, most appointed privacy regulators operate in a reactive way. While this is a completely acceptable method of operation, it is not the most efficient. Research has shown that most data leaks containing personal information remains available for more than a month on average before being detected and reported. Quite often the data is discovered by a third party who selects to notify the responsible organization but can just as easily copy the data and make use of it. This paper will display the potential benefit a privacy regulator can expect to see by implementing pro-active detection of electronic personally identifiable information (PII). Adopting pro-active detection of PII exposed on public networks can potentially contribute to a significant reduction in exposure time. The results discussed in this paper were obtained by means of experimentation on a custom created PII detection system.

Swart, I. P., B. Irwin, and: M. M. Grobler "*Towards a platform to visualize the state of South Africa's information security*" *Information Security for South Africa, 2014*. IEEE, 2014.

Abstract

Attacks via the Internet infrastructure is increasingly becoming a daily occurrence and South Africa is no exception. In response, certain governments have published strategies pertaining to information security on a national level. These policies aim to ensure that critical infrastructure is protected, and that there is a move towards a greater state of information security readiness. This is also the case for South Africa where a variety of

policy initiatives have started to gain momentum. While establishing strategy and policy is essential, ensuring its implementation is often difficult and dependent on the availability of resources. This is even more so in the case of information security since virtually all standardized security improvement processes start off with specifying that a proper inventory is required of all hardware, software, people and processes. While this may be possible to achieve at an organizational level, it is far more challenging on a national level. In this paper, the authors examine the possibility of making use of available data sources to achieve inventory of infrastructure on a national level and to visualize the state of a country's information security in at least a partial manner

---

Swart, I. P., M. M. Grobler, and Irwin, B: "*Visualization of a data leak*."
Information Security for South Africa, 2013. IEEE, 2013.

Abstract

The potential impact that data leakage can have on a country, both on a national level as well as on an individual level, can be wide reaching and potentially catastrophic. In January 2013, several South African companies became the target of a hack attack, resulting in the breach of security measures and the leaking of a claimed 700000 records. The affected companies are spread across a number of domains, thus making the leak a very wide impact area. The aim of this paper is to analyze the data released from the South African breach and to visualize the extent of the loss by the companies affected. The value of this work lies in its connection to and interpretation of related South African legislation. The data extracted during the analysis is primarily personally identifiable information, such as defined by the Electronic Communications and Transactions Act of 2002 and the Protection of Personal Information Bill of 2009.

M Grobler, I Swart - ICT and Society, 2014. "*On the Probability of Predicting and Mapping Traditional Warfare Measurements to the Cyber Warfare Domain"*. Springer Berlin Heidelberg

Abstract

Cyber warfare is a contentious topic, with no agreement on whether this is a real possibility or an unrealistic extension of the physical battlefield. This article will not debate the validity and legality of the concept of cyber warfare, but will assume its existence based on prior research. To that end the article will examine research available on traditional warfare causes, elements and measurement techniques. This is done to examine the possibility of mapping traditional warfare measurements to cyber warfare. This article aims to provide evidence towards the probability of predicting and mapping traditional warfare measurements to the cyber warfare domain. Currently the only way of cyber warfare measurement is located in traditional information security techniques, but these measurements often do not adequately describe the extent of the cyber domain. Therefore, this paper aims to identify a set of criteria to aid in the prediction of cyber warfare probability.