Cyber threat intelligence practices in the national sphere of government in South Africa

Lucia Masilela (a) Danielle Nel-Sanders (b)*

(a) School of Public Management, Governance and Public Policy, College of Business and Economics, University of Johannesburg, Johannesburg, South Africa.
(b) Professor, School of Public Management, Governance and Public Policy, College of Business and Economics, University of Johannesburg, Johannesburg, South Africa

Abstract

Over the past two decades, cybercrime and cybercriminals have had a great impact on the safety, security and protection of the public sector’s confidential data and information assets. The increased usage of the internet and new, advanced 4IR technologies, and the digitisation of government’s public sector goods and services have become a growing concern to the government and its public sector institutions. In the South African context, as a developing country it unfortunately lags behind advanced and developed nations in terms of fully counteracting cybercrime and cybercriminal operations. Despite this challenge, the South African government has been making tremendous efforts in combating cybercrime. The aim of this article is to contextualise the study and practice of cyber threat intelligence at the national sphere of government in the South African public sector, namely, the former Department of Energy (DoE), former Department of Science and Technology (DST) and the former Department of Environmental Affairs (DEA) a qualitative research approach was followed using a case study approach. Primary data was collected through semi-structured interviews with senior departmental management. The findings are presented according to the Threat Intelligence Lifecycle analysis which serves as an analytical framework. The study concludes that in order to achieve effective cybersecurity practices and principles in the public sector, the government must identify the top trends commonly associated with cybersecurity in order to be able to develop and implement counteractive strategies and approaches, as well as to improve security systems and programs to ensure that an organisation is sufficiently prepared for and protected against cybercriminals and cyberattacks.

Keywords:
Government Data and Information
Security Systems, Cybersecurity,
Cyber threat intelligence, Cyber risks

JEL Classification:
M38

Introduction

The utilisation of advanced technologies has resulted in an increase in cybercriminal activities, which have complicated, challenged, and interrupted cyber security roles, responsibilities, and the functional and operational activities in public sector institutions. The practice and study of data and information security and the protection of both digital and physical infrastructure in the public sector has become an increasingly important field of study for the government and its public sector institutions.

There is current a need to enhance and improve on current DISG practices and principles in order to effectively mitigate the prevalence of increasing data- and information-related crime, security risks, and challenges in government institutions (Moulton and Coles 2003:45-52; IT Governance Institute 2003:15-21). This has been evident when there are sudden “leaks” or “anonymous” tip-offs that have made it onto the front pages of well-known newspapers. This leakage of information has often been found to be associated with direct attempts by individuals to harm the reputation of an organisation or well-known public officials. The misuse of personal data and information, as well as private documents belonging to an organisation, can have damaging ramifications,
especially if the information has been distorted in order to create a tarnished perception in order to create a harmful outcome to a particular situation (Moulton and Coles 2003:45-52; IT Governance Institute 2003:15-21).

As a result, public sector institutions have found themselves to be victims of the influx of cybercriminal behaviour and activities. Public sector institutions have made significant contributions to improving the security of their public sector data and information (PSDI) assets through various DISG practices and tools driven and guided by the power and infrastructure of advanced information and communication technology (ICT) as centralised platforms.

The study focuses on contextualising the study and practice of cyber threat intelligence and how it can be incorporated into the South African national sphere of government for improved DISG management practices, Firstly, this article will provide a contextual background to the study. Secondly, the concepts of cybercrime and cyberterrorism will be conceptualised. Thirdly, this article will provide a discussion on cybercrime and cybersecurity challenges within the broader African context. Fourthly, this article will provide a discussion on the theory and practice of cyber threat intelligence. Fifthly, this article will discuss the methodological approach to the study which consisted of a qualitative research approach. Sixthly, the research results are discussed by analysing the cybersecurity and cybercrime landscape in the national level of government in South Africa and analysing the dataset through systematic threat intelligence lifecycle analysis, which serves as an analytical framework for the qualitative data analysis. Lastly, the article will provide conclusions and recommendations of the study.

**Contextual background to the study**

Cybercrime in developing countries has been a growing concern for both public and private sector institutions. Governments, private sector institutions, citizens, international bodies, and various other stakeholders have found it challenging to identify and implement strategic and effective DISG strategies to combat cybercrime in developing countries. Developing countries have been found to lack the advanced technological capabilities, skill sets, and experience to aggressively tackle cybercriminal attacks through DISG approaches. Combating cybercrime requires extensive periods of research and large financial investments into equipping developing countries with the necessary capabilities that will allow them to identify and implement strategic DISG practices for the protection of critical data and information assets. In developing countries, the fight against cybercriminals and cyberattacks has been relatively challenging due to the inherent impacts of social, political, and economic environmental factors. Therefore, as a result of the measures required to implement and ensure the technical protection of critical PSDI assets, it has been found to be a cost-intensive approach to developing nations that have emerging or semi-developed economies (Davis and Ranchod 2017:2; Wolfpack Institutional Risk (Pty) Ltd 2016:10; KPMG 2017:7). A major challenge that developing countries are often faced with is the lack of efficient and effective policies on cybercrime, as well as effective DISG management systems and approaches in their respective regions. Governments in developing countries have been found to be experiencing challenges in their efforts to identify, establish, and implement effective regulatory policies and legislation that can aggressively counteract cybercrime while adequately protecting their critical PSDI assets. These elements have stagnated developing countries’ capabilities in terms of formulating and implementing integrated and protective measures in order to tackle cybercrime, as well as ensuring their sustainable and long-term goals and objectives towards effective cybersecurity measures through improved DISG approaches (Davis and Ranchod 2017:7-8). In the African context, 4IR technologies promote increased economic growth, new and improved skill sets, societal development, improved ICT infrastructure, new businesses, and entrepreneurial opportunities for small and medium enterprises. These new opportunities and possibilities for innovative products and services have led to a tremendous increase in Internet usage, which has also resulted in increased vulnerability to cyber risks and attacks (Davis and Ranchod 2017:2; Wolfpack Institutional Risk (Pty) Ltd 2016:10; KPMG 2017:7).

**Conceptualising Cybercrime and Cyberterrorism**

Due to the latest developments in the third industrial revolution (3IR) and fourth industrial revolution (4IR), organisations in public and private sectors have been placed in a position to deal with increased cyber risks and instances of crimes (Van der Merwe, Roos, Pistorius and Eiselein, 2008:61; Brickey, 2012:1; PwC, 2016:25-26). The full advancement into the Internet of Things has resulted in organisations conducting daily activities and functions through the use of advanced technologies and capabilities to improve the delivery of services and products to consumers. South Africa as a developing nation has become more exposed to the use of advanced technologies, particularly through the use of ICT and modern state infrastructure. This has allowed citizens, the government, private businesses, and various other stakeholders to interact and become more connected than ever before due to this widespread use of the Internet. South Africa has been described as a low- and middle-income economy, which has implemented progressive approaches to position itself to benefit from the rapid and accelerated technological developments that can help tackle unemployment by unlocking economic growth and societal development (Accenture, 2015:7). This widespread use of ICT and the Internet has improved economic and societal growth and development. It has, however, also introduced South Africa to new and uncertain vulnerabilities in the cyber domain, which inevitably undermined the country’s efforts towards effective cybersecurity efforts for improved DISG practices and principles. Hackers are developing and using advanced technologies, programs, and software to engage in criminal activities such as identity theft, fraud, robbing financial institutions, and hacking into private and confidential state and corporate organisations to steal information (Rudner, 2013:467; Wolfpack Institutional Risk (Pty) Ltd, 2016:10; KPMG, 2017:7).
Defining and Conceptualising Cyber Threat Intelligence

The data and information security systems utilised by organisations all over the globe have over the past decade become exceptionally vulnerable and are constantly under attack from cybercriminal individuals and organisations. These cybersecurity challenges, threats and risks have therefore compromised the integrity, reputation and security principles and practices of both private and public sectors organisations. Cyber threat intelligence has therefore been identified as a holistic and integrated approach towards cyber threats and cybercriminal behaviour (Tounsi, 2019:2). Threat intelligence also referred to as Cyber Threat Intelligence (CTI) can therefore be described as all processes related to the collection, processing and analysing of information regarding the adversaries and vulnerabilities within cyberspace in order to disseminate actionable threat intelligence to counteract those adversaries and vulnerabilities by thoroughly understanding the motivations, methods and techniques utilised by cybercriminals and thus developing and implementing strategies to successfully mitigate cyber security risks, uncertainties and vulnerabilities (National Cyber Security Centre (NCSC), 2019:6). CTI therefore allows organisations to place themselves in a proactive position towards cyberthreats and risks, thus increasing their visibility by being able to detect and prevent threats before their materialisation and preventing any negative or catastrophic consequences to an organisation. CTI when conducted correctly provides essential reinforcing defences towards an organisation’s Information Technology (IT) infrastructure, thus making a proactive security ecosystem for all the organisation’s technological and digital systems, processes and infrastructure. This therefore strengthens senior organisational management’s decision-making processes towards cybersecurity strategies and approaches (Zhao, Yan, Li, Shao, He, Li, 2020:95).

The Importance and Significance of Gathering Good Intelligence

Good intelligence can therefore be described as a process that involves the collection and utilisation of accurate, reliable and unbiased data and information that will enable an organisation’s security professionals to fully and thoroughly understand the threats, risks and uncertainties that could materialise from cybercriminal behaviour and techniques. Good threat intelligence therefore gives cyber security professions a comprehensive analysis and overview of what risks could occur; where these risks and threats are coming from; how the risks and threats could materialise; and what damages and repercussions these could have on its security systems and infrastructure and the overall organisation (Ozkaya, 2022:47). Good intelligence therefore ensures a higher feasibility and viability of building very strong and sufficient cyber security defence mechanisms, thus resulting in proactive cyber security measures.

The Different Levels of Cyber Threat Intelligence

In order for CTI practices to be effective towards cyber threats, risks, uncertainties and cybercriminal behaviour, an organisation’s senior management must therefore thoroughly design, implement and sustain CTI functions and practices that add integrated and holistic cybersecurity measures throughout the organisation. The theory and institutionalisation of CTI is based on the practices of proactive security measures. For the purposes of this article four CTI levels in which an organisation can achieve good threat intelligence have been identified. These good threat intelligence variables can be divided into four categories, which include: strategic threat intelligence; tactical threat intelligence; operational threat intelligence; and technical threat intelligence. The four variables of threat intelligence are grouped together but are in no way a sequential set of variables to follow when analysing the different levels of cyber threat intelligence. However, for best practices it is advised that these four variables be analysed and assessed concurrently in order to ensure the holistic cyber threat intelligence practices for an organisation.

Figure 1: Different Levels of Cyber Threat Intelligence; *Source:* Author’s own illustration
Strategic Threat Intelligence

The first category is strategic threat intelligence. Strategic threat intelligence intends to provide the organisation with high-level quality information regarding its security measures and the posture of the organisation from a strategic point of view. Strategic threat intelligence provides a holistic analysis of all the threats, risks and challenges the organisation are likely to be faced with in the event that there is a security breach or incident; the types of cyber-attacks and criminal behaviours; the possible impacts of those identified risks, threats and uncertainties; and the impact of those risks, threats and uncertainties of the strategic activities, goals and objectives which could impact on the existence and continuation of the organisation (Ozkaya, 2022:49-50). Strategic threat intelligence is primarily a function associated with high-level executives and management within an organisation’s IT roles, functions and responsibilities. Top-level management is therefore tasked with the responsibility of evaluating all relevant information sources regarding the cyber risks involved; the unknown and uncertain future of cyber risks, threats, and challenges; and the impact of these cyber risks, threats and uncertainties on the organisation’s reputation (Chisman and Ruks, 2015:6). Strategic threat intelligence provides senior management with a comprehensive report of the long-term impacts of cyber security risks, threats and uncertainties on the organisation in the event of materialisation. Once this report has been reviewed and assessed by senior management, its response would be long-term strategic threat intelligence countermeasures through predictive insights and tools. The long-term strategic threat intelligence countermeasures must ensure the protection of all IT infrastructure, systems and processes; the organisation’s internal and external customers, stakeholders, partners, investors and suppliers; and the organisation’s employees who make daily use of ICT processes, systems, and infrastructure. Strategic threat intelligence not only provides insights regarding cybersecurity risks, threats and countermeasures it is also utilised towards key decision-making processes regarding the allocation of monetary and non-monetary resources towards other organisational assets and processes that may be interrelated and impacted by cybersecurity attacks and incidents (Ozkaya, 2022:49-50).

Tactical Threat Intelligence

The second component is tactical threat intelligence. Tactical threat intelligence primarily focuses on protecting the organisation’s assets and resources from potential cyber threats, attacks, risks and uncertainties. Tactical threat intelligence provides intel regarding the type of attackers that could potentially target the organisation; the cyber tactics and tools that could be utilised; and the motivations that these cyber-attacks and criminal behaviours are founded on. Cybercriminals will always attempt to steal and infiltrate security systems and infrastructure with a particular target and goal in mind, which could for example include financial benefits such as holding the organisation hostage by withholding certain types of data and information from accessibility and useability and thus demanding ransom money or it could be politically motivated based on the theories of cyber terrorism (Ozkaya, 2022:50-51). Tactical threat intelligence is therefore in most cases utilised by middle or next-level managers within an organisation such as IT service managers, network operators, architects, administrators, and security operations managers. Tactical threat intelligence provides in-depth information regarding: the potential attack(s); the capabilities and strengths of the cyber attackers; the magnitude of the cybersecurity threat(s), risk(s) or challenge(s); the type and level of vulnerabilities this could have on the organisation; and the types of systems that are most likely targeted and infiltrated (Chisman and Ruks, 2015:7). This information is then utilised by middle- and next-level management to develop and implement the necessary defence systems and mechanisms to ensure the protection of an organisation’s security systems and infrastructure from cyber-attacks, threats and risks. There are a number of sources that middle- and next-level management can utilise to develop tactical threat intelligence. These can include: incident reports, malware and phishing reports; security campaign reports; human intelligence and attack group threat reports; technical papers on white papers on cybersecurity threats, risks and challenges; cybersecurity manuals and research reports; cybersecurity forensic reports; and third-party sources such as research consulting firms and various other credible and reliable sources (Ozkaya, 2022:50-51).

Operational Threat Intelligence

The third component is operational threat intelligence. Operational threat intelligence relates to all the information regarding the operationalisation of an organisation on a day-to-day basis. The details and information gathered from operational threat intelligence primary deal with the analysis of all factors that could go wrong and could be impacted by a cybersecurity threat, risk or uncertainty that could negatively impact on the operational capacity of the organisation to perform its functions. The data and information gathered at an operational perspective is designated to reveal the risks and threats that the organisation could experience. In addition, the operational threat intelligence will further reveal insights regarding the various types of methodologies that cyber attackers utilise when attempting to compromise and infiltrate the operations of an organisation (Chisman and Ruks, 2015:6). Operational threat intelligence will include historical data and information regarding previous cybersecurity threats, risks, uncertainties and challenges that were experienced by the organisation and changes in the organisation’s security processes and controls that could have provided a vulnerability within which a cyberattack, risk or uncertainty could materialise and cause security lapses (Ozkaya, 2022:51-52). Operational threat intelligence intends to help the organisation to identify and understand threats that could impact on operations; the capabilities of cybercriminals and cyberattacks to seriously harm and compromise its operational functionality; to identify the most vulnerable operational assets that could be of significant interest to cyber hackers and cybercriminals; and a comprehensive assessment of all the opportunities in which a cyber hacker could infiltrate to gain access to organisational systems. Once the operational threat intelligence has been collected and analysed an organisation’s security professionals are then tasked with systematic and consistent efforts of developing, implementing, upgrading and remodelling cybersecurity measures, practices and
systems in an effort to create and instil difficulties for cyberhackers to prevent them from infiltrating its cyber defence walls (Ozkaya, 2022:51-52).

Technical Threat Intelligence

The last variable is technical threat intelligence. Technical threat intelligence focuses on providing intel on the type and magnitude of the cyber attacker’s resources, cyber hacking capabilities as well as the means of infiltrating the organisation’s IT systems and infrastructure. The details that technical threat intelligence make available to an organisation are often very limited in terms of their lifespan, scope and viability as opposed to strategic and operational threat intelligence as these cyber hackers and criminals are therefore quick in changing their techniques, targets, and resources to infiltrate cybersecurity systems belonging to an organisation. Technical threat intelligence aims to enable an organisation’s security team to rapidly respond and counteract all and any cybersecurity threats, risks and challenges that emerge through its intelligence mechanisms (Chisman and Ruks, 2015:7). Technical threat intelligence is designed to enable and supply an organisation’s security professionals with rapid response strategies in order to eliminate as effectively as possible any and all targeted cyber security threats, risks, uncertainties and challenges. Technical threat intelligence also makes use of external feeds and sources to gain better insights into cybercriminal behaviours, tactics and patterns, thus positioning the organisation into a proactive approach towards developing and implementing high-quality, standardised and effective and deliverable cybersecurity measures and practices. Based on the developed security software and infrastructure of an organisation, technical threat intelligence will therefore provide senior management with additional cyber security risk and threat indicators, thus allowing them to enhance security measures against cyber breaches. In addition, technical threat intelligence can assist in identifying malicious IP addresses that are feeders of cybersecurity risks and threats and the identification of attackers based on their geographical irregularities. The technical threat intelligence gathered here can therefore provide an organisation’s security professionals with intel that can be used to develop security measures that can identify and block inbound or outbound traffic used by cybercriminals to access an organisation’s digital systems and processes (Ozkaya, 2022:52-53).

Research and Methodology

The chosen methodological approach for this research study was a qualitative research approach. Qualitative data analysis provides answers to research questions in the form of rich descriptions through synthesised information in order to present in-depth meaning. The data presented in this article is based on semi-structured interview questions. The interview results and interpretations are derived from the semi-structured interview questionnaire that was developed which consisted of 29 questions that were subcategorised into four sections. The semi-structured interviews were aimed at identifying, analysing, investigating and understanding the cybersecurity practices, principles and processes that have been applied and institutionalised by senior management in government to ensure effective and efficient cybersecurity measures against cybercrime and cyberattacks within the respective departments. The interview data for this study were collected through one-on-one interviews with senior management in the ministries of energy, science and technology and environmental affairs, namely the Department of Energy (DoE), former Department of Science and Technology (DST) and the former Department of Environmental Affairs (DEA). A two-phased approach to sampling was followed, the first was sampling method was snowball sampling. Snowball sampling can be defined as a technique/strategy that a researcher uses in order to find research participants. The use of snowball sampling in interviews gives researchers an opportunity to make new discoveries that may add more value and depth to the research study. The second sampling method that was utilised was purposive sampling. The choice of this type of sampling is intended to identify and use particular participants who possess the types of characteristics that are relevant and informative to the research study. Fourteen participants were interviewed as skilled, knowledgeable and experienced personnel who specialise in the area of cybersecurity practices in their respective departments. The research results were analysed using a Threat Intelligence Lifecycle analysis from the study and practice of cyber threat intelligence in the ICT discipline. The Threat Intelligence Lifecycle analysis consists of a six-step process which includes: planning and direction; collection, processing; analysis, dissemination; and feedback. This therefore provided a systematic and iterative process and analysis of the data set.

Furthermore, the threat intelligence lifecycle process was therefore utilised as an analytical framework. In addition, the six-step process utilised the headings to thematise the dataset into primary themes and subthemes which are presented in a tabulated form. The interview responses are analysed using thematic analysis. In qualitative research, thematic analysis can be used as a method to analyse present classifications, themes, and patterns that are relevant and related to the raw data that were collected during the research process. The research results discussed in this article are presented thematically according to the threat intelligence lifecycle analysis, which is thoroughly discussed in this article.

Table 1 illustrates the various levels of government in the South African government. This study focuses on the national level of government.
Table 1: The Three Levels of Government

<table>
<thead>
<tr>
<th>Level</th>
<th>Functions</th>
<th>Legislature administered by:</th>
<th>Executive administered by:</th>
<th>Administration performed by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>National</td>
<td>Formulation and approval of laws, policies, and Bills for provincial and local municipalities</td>
<td>Parliament</td>
<td>President</td>
<td>Director General (DGs), Deputy Director General (DDGs), Chief Director (CDs), and government chief officers (GCOs)</td>
</tr>
<tr>
<td>Provincial</td>
<td>Coordinating, monitoring, evaluating and supporting municipalities in each province</td>
<td>Legislature</td>
<td>Premier and Executive Council</td>
<td>Heads of Departments (HoDs), middle- and lower-level managers and staff</td>
</tr>
<tr>
<td>Local</td>
<td>Approval of by-laws for their districts</td>
<td>Council</td>
<td>Mayor and Mayoral Committee</td>
<td>Municipal manager, HoDs and staff</td>
</tr>
</tbody>
</table>

Source: Author’s own construction

For the primary goals and purposes of this article, the national sphere of government was selected. In order to determine the sample size from Table 1, this study therefore considered the national sphere of government, specifically in terms of its administrative functions, because it consists of DGs, DDGs, CDs, and GCOs who are primarily responsible for managing and overseeing all administrative roles, functions, and responsibilities for DISG in the national sphere of government.

Research Findings

The following section of this article will analyse the various cybersecurity practices that have been institutionalised in three National governments, namely, the DoE, DST and the DEA. The data presented in this section are the results and findings of a research study undertaken for a master’s dissertation. The interview results and interpretations discussed below do represent a generalisation of the interview data.

The Threat Intelligence Life Cycle

The development and institutionalisation of intelligence from a cybersecurity perspective is a knowledge-based process that involves the analysis of raw data sources into completed information assets that can be utilised towards the preparation of cybersecurity practices and principles for an organisation’s security professionals. The generation of threat intelligence emerges from a cycle that intends to convert raw data into useful intelligence that can be used to improve the posture and position of an organisation to proactively target and handle cybersecurity threats, risks, uncertainties and challenges. The threat intelligence cycle has been identified as an iterative process that can be followed by an organisation’s cybersecurity personnel to make use of intel to generate knowledge that is clearly refined that will identify problem areas in the scope of threats, risks, uncertainties and challenges of cybersecurity. The threat intelligence lifecycle aims to provide improvements towards cybersecurity on an iterative process. The threat intelligence lifecycle consists of a six-part process, which includes: planning and direction; collection; processing; analysis; dissemination; and feedback. Figure 2 below provides an illustration of the threat intelligence lifecycle that begins with planning and direction and ends with feedback. The illustration presents how each step is feeding from the previous step into the next, indicating the interconnectedness and relationship between each variable. The threat intelligence cycle will further be utilised as an analytical framework for assessing cybersecurity practices, principles and processes within the DEA, DSI and DoE. The purpose of utilising the six-step life cycle analysis was to identify what types of cybersecurity principles, practices, tools, techniques, strategies and policies will emerge, thus thematising the findings into themes according to the threat intelligence lifecycle analysis.
Figure 2: Threat Intelligence Cycle; Source: Author’s own illustration

Step One: Planning and Direction

The first step in the six-part process is planning and direction. In the process of acquiring and producing intel on threat intelligence the right questions should be asked to the right people and for the right reasons. Planning and direction requires focusing on a single issue, event, incident, fact and activity. Security professionals must therefore avoid open-ended questions and scenarios that will result in unclear and undefined answers, resulting in a vague and broadened direction towards the necessary cybersecurity measures that are needed. The key guiding factor within this step is determining who these cybersecurity measures will benefit and how it will benefit them (CyberEdge Group, LLC, 2018:3-4; Ozkaya, 2022:53).

Step Two: Collection

The second step is the collection of cybersecurity data and insights. This step consists of gathering all the necessary raw data from both internal and external sources that could be turned into viable, factual and unbiased information. Internal sources of data collection include risk registers, threat event logs, records of security breaches, network servers, IT infrastructure, email communications, search history records, system vulnerabilities, compromised passwords as well as past incident response reports. External sources of data include open web searches, third-party vendors, malware, phishing attacks, the dark web and hacker threats, and theft of digital devices and infrastructure to mention a few (CyberEdge Group, LLC, 2018: 4-5; Ozkaya, 2022:53).

Step Three: Processing

The third step is processing the internal and external data collected from the previous step. This step entails the sorting, classification, categorising and organising of the data through the use of metadata tags, filtering the data, and identifying and getting rid of repetitive and redundant information as well as identifying and verifying false positives and negatives of cybersecurity information (CyberEdge Group, LLC, 2018:6; Ozkaya, 2022:53).

Step Four: Analysis

The fourth step is analysing the threat intelligence intel. The primary goal and purpose of this step is to inform an organisation’s cybersecurity personnel of what type of threat intelligence it has. The threat intelligence in this step can consist of a list of all the current and past cybersecurity threats, risks and breaches; the types of digital systems and infrastructure that are most targeted; the motivations of the cybercriminals and criminals attempting to hack their systems; the type of tools, software and techniques that cybercriminals and hackers use; the geographical locations of cyberattacks from IP addresses and various other intelligence intel that can be of necessity to the organisation’s cybersecurity personnel (CyberEdge Group, LLC, 2018:6;-7 Ozkaya, 2022:54).

Step Five: Dissemination

The fifth step consists of disseminating the threat intelligence intel and then determining its targeted audience, as the cybersecurity intel will vary based on its cybersecurity needs, strategies, as well as operational goals and objectives within an organisation. An important element within the threat intelligence lifecycle is “tracking” the cybersecurity intel for example: who it must be sent to; why is it sent; what is its purpose; what is the intended goals of sharing this intelligence and most importantly how it will be utilised to manage cybersecurity risks, threats, uncertainties and challenges. Tracking the dissemination of the cybersecurity intel ensures the continuity between the different phases of the threat intelligence lifecycle, thus being able to verify and know who has the intelligence, what level of progress it is at and what findings have emerged towards cybersecurity defence strategies and approaches. This therefore
ensures the integration of the threat intelligence cycle in between and across its phases (CyberEdge Group, LLC, 2018:7; Ozkaya, 2022:54).

**Step Six: Feedback**

The final step in the threat intelligence lifecycle is feedback. Feedback plays an important role in the threat intelligence lifecycle as it loops and feeds back into step one, which is the planning and direction phase of the cycle. The feedback that is communicated within this step will initially be threat intelligence intel that the organisation will base its next cybersecurity processes and findings on for the next emergence of cyber risks, threats and challenges. The feedback phase should consist of constructive feedback that is both positive and negative to be used to enhance and improve on current and future cybersecurity practices and principles. This step will also consist of all the measures directed at improving the practicality and feasibility of cybersecurity measures, such as training and awareness sessions; security performance plans and indicators; the development of security tools and techniques; and the types of committees and personnel that will be assigned with the responsibility of enhancing and ensuring the feasibility of cybersecurity practices. In addition, this feedback step will also allow for the opportunity to identify and discuss what cybersecurity practices do not work and deliver effective cybersecurity defences; and what methods and approaches could be applied to counteract vulnerabilities and ensure maximum feasibility of cybersecurity practices and principles (CyberEdge Group, LLC, 2018:8; Ozkaya, 2022:55).

Table 2 below presents a tabulation of the themes that emerged through the use and application of the threat intelligence lifecycle and its six-part process. The left-hand side of the table consists of all the headings of the six-part process and on the right-hand side the table consists of all the themes that emerged from analysing the various cybersecurity measures, practices, tools, polices, cyber threats and risks, frameworks, strategies, cybersecurity personnel and committees. The primary goal of using the threat intelligence lifecycle was to determine whether or not these cybersecurity practices and principles could be found across and in between the DEA, DoE and DSI. Table 2 below tabulates the consolidated cybersecurity practices that can be found in each step of the six-part process.

**Table 2: Threat Intelligence Lifecycle: Consolidated Analysis of the DEA, DSI and DoE**

<table>
<thead>
<tr>
<th>Threat Intelligence Lifecycle</th>
<th>Variables / Themes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Planning and Direction</strong></td>
<td>ICT Security Policy</td>
</tr>
<tr>
<td></td>
<td>Enterprise Content Management Policy</td>
</tr>
<tr>
<td></td>
<td>Email, Intranet and Internet Policy</td>
</tr>
<tr>
<td></td>
<td>Computing Asset Replacement Policy</td>
</tr>
<tr>
<td></td>
<td>Infrastructure Protection Policy</td>
</tr>
<tr>
<td></td>
<td>Security Policy</td>
</tr>
<tr>
<td></td>
<td>Security Organisation and Classification Policy</td>
</tr>
<tr>
<td></td>
<td>IT Security Policy</td>
</tr>
<tr>
<td></td>
<td>Physical Security Policy</td>
</tr>
<tr>
<td></td>
<td>Asset Management Policy</td>
</tr>
<tr>
<td></td>
<td>Records Management Policy</td>
</tr>
<tr>
<td></td>
<td>Standard Operating Procedure Policy</td>
</tr>
<tr>
<td></td>
<td>Information Security Policy</td>
</tr>
<tr>
<td></td>
<td>Firewall Policy</td>
</tr>
<tr>
<td></td>
<td>Backup Policy</td>
</tr>
<tr>
<td></td>
<td>Logical Access Policy</td>
</tr>
<tr>
<td></td>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td><strong>Collection</strong></td>
<td>IT Systems</td>
</tr>
<tr>
<td></td>
<td>Internal System</td>
</tr>
<tr>
<td></td>
<td>Access Control Systems</td>
</tr>
<tr>
<td></td>
<td>Mobile Device Management Programme</td>
</tr>
<tr>
<td></td>
<td>Electronic Document Management Systems</td>
</tr>
<tr>
<td></td>
<td>Email Archiving Solution</td>
</tr>
<tr>
<td></td>
<td>Enterprise Content Management System</td>
</tr>
<tr>
<td></td>
<td>Document Management System</td>
</tr>
<tr>
<td></td>
<td>File Plan System</td>
</tr>
<tr>
<td></td>
<td>H-Drive Online Backup System</td>
</tr>
<tr>
<td></td>
<td>Daily Backups</td>
</tr>
<tr>
<td></td>
<td>Weekly Backups</td>
</tr>
<tr>
<td></td>
<td>Monthly Backups</td>
</tr>
<tr>
<td><strong>Processing</strong></td>
<td>Collection of Data and Information Assets</td>
</tr>
<tr>
<td></td>
<td>Classification of Data and Information Assets</td>
</tr>
<tr>
<td></td>
<td>Storage of Electronic and Physical Assets</td>
</tr>
<tr>
<td></td>
<td>Accessible Data and Information Assets</td>
</tr>
<tr>
<td></td>
<td>Readable Data and Information Assets</td>
</tr>
<tr>
<td></td>
<td>Transferable Data and Information Assets</td>
</tr>
<tr>
<td></td>
<td>Email Communication</td>
</tr>
<tr>
<td></td>
<td>Telephonic Communication</td>
</tr>
</tbody>
</table>
### Table cont’d

| Environmental Data and Information Security |
| Research Reports |
| Financial Budgets Reports |
| Strategic Plans |
| Financial Data |
| Citizen Data |
| Security Planning |
| Monitoring and Evaluating |
| Feedback Reports |
| Supply Chain Partners |
| Contractual Agreements |
| Private Sector Business |
| Private Investors |
| Identification Numbers |
| Cabinet Memos |
| SSA |
| Vetting Process |
| Classification of Access |
| Classification Levels |
| Classification of Documents |
| Declaration of Secrecy |
| Non-Disclosure Forms |
| Vetting Certification |
| Security Clearance |
| Security Clearance Certificates |
| Top-Secret Classifications |
| Secret Classifications |
| Confidential Classifications |
| Classified Classifications |
| Sensitive Classifications |
| Cabinet Member Secrecy |
| Other Types of Classifications |

### Analysis

| Violation of Policies |
| Violation of Legal Obligations |
| Violation of Regulatory Requirements |
| Violation of Contractual Agreements and Obligations |
| Reputational Risks |
| Financial Losses |
| Capacity Challenges |
| Loss of Data and Information Assets |
| Reputational Damage |
| Loss of Integrity |
| Loss of Trust and Transparency |
| Electronic Threats / Attacks |
| Security Risks |
| Security Challenges |
| Security Threats |
| Security Breaches |
| Breach of Communication |
| Large-Scale Power Outages |
| Fraud and Corruption |
| Fraudulent Activities |
| State Security |
| Unauthorised Access |
| Loss of Tacit Information and Knowledge |
| Malicious Virus Attacks |
| Phishing Attacks |
| Viral Attacks |
| Cyberattacks |
| Hacking |
| Denial of Access Virus |
| Loss of Institutional Memory |
| Malicious Virus Attacks |
| Cybercriminal Activities |
| Unauthorised Access |
| Bridge/Theft of Critical Data and Information Assets |
| Tacit Information and Knowledge |
The South African policy context for Cyber Security and Threat Intelligence

One of the most important functions of the government is to maintain the trust, protection, secrecy, and privacy of data and information assets that belong to its citizenry. National, provincial, and local government spheres are constantly collecting, sorting, classifying, and storing data and information assets. Managing such voluminous data and information assets can become a complicated task even for some advanced governments. At the peak of the 3IR, South Africa was identified as one of the top three countries (the other two being the USA and the UK) that experienced massive increases in Internet vulnerabilities, cybercrime, and cyberattacks that threaten the country’s national security (RSA 2011:11). As a response to this, South Africa engaged in various activities with the aim of combatting cybercrime and cyberattacks. These activities included cybersecurity awareness and training programmes to create vigilance of cybercriminal activities that employees should be aware of in the workplace. The South African government realised that it cannot continue to function without a definite national cybersecurity policy and that measures must be put in place to adequately protect the country’s critical data and information assets through improved cybersecurity management practices (RSA 2011:11). In the South African context, cybersecurity initiatives are often complex and multidimensional, with the aim of accommodating and integrating all the necessary cybersecurity requirements. Table 3 provides a summary of the legislative policies that have been developed and implemented towards cybersecurity and threat intelligence practices. The legislative frameworks tabulated below in Table 3 have been identified as the current and existing legislative frameworks in South Africa for cybersecurity and threat intelligence. These legislative frameworks have therefore been institutionalised as a foundational basis for the overall cybersecurity and threat intelligence practices within each government department and must be adhered to at all times when dealing with cybersecurity risks, threats, uncertainties and challenges.

Source: Author’s own illustration
Table 3: Legislative Frameworks for Cybersecurity and Threat Intelligence

<table>
<thead>
<tr>
<th>Legislative Framework Variables</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Information Security Standards (MISS) of 1996;</td>
<td>The primary goal and purpose of the MISS is to ensure that the government caters for the security interests and requirements of South Africa through counter-intelligence measures and procedures. The MISS are contained in an information security document that stipulates standards and guidelines regarding the minimum-security measures that organisations both in the private and public sectors must implement in order to adequately protect their sensitive, critical, or classified information assets. MISS includes Chapter 3: the Provision and Application of Security Measures; Chapter 4: Document Security; and Chapter 5: Personnel Security (RSA 1996).</td>
</tr>
<tr>
<td>SITA Act, No. 88 of 1998 (as amended by Act 38 of 2002 [RSA 2002b]);</td>
<td>The primary goal and purpose of the SITA Act is to provide rules and regulations regarding the establishment of an organisation / company that will be responsible for the provision of ICT services to the public administration of South Africa. Subsection 6 stipulates the measures related to the maintenance of information security systems to the departments and other public bodies; Subsection 7 stipulates the development, implementation and sustaining of a conducive and comprehensive information security environments for departments in order to satisfactorily utilise ICT in a safe and enabling environment; Subjection 9 stipulates the regulations related to protecting data and information authentication, processing, duplication and deletion processes; and Subsection 23 and 24 stipulates the regulation of procurement processes and requirements for information security systems that must be oversee and approved by the Minister of Intelligence (RSA 1998; RSA 2002b).</td>
</tr>
<tr>
<td>Minimum Information Interoperability Standards (MIOS) of 2001;</td>
<td>The purpose of the MIOS is to provide the public sector with prescribed open systems standards that will ensure minimum levels of interoperability within the Information Security and ICT systems that are utilised to conduct government functions as well as minimum interoperability levels in relation to industry, citizens and the international communities that government engages and operates with. In addition, the MIOS provides a framework to ensure compliance; provides guidelines and a basis for designing, using and implementing open standards and solutions for Information Security; verification and certification processes for the conformance of Information Security and ICT goods and services; and provides guidelines for the integration MIOS compliant products into Government Information infrastructure.</td>
</tr>
<tr>
<td>Electronic Communications and Transactions (ECT) Act, No. 25 of 2002</td>
<td>The ECT Act has a total of 14 chapters; the following chapters within in ECT Act therefore discuss regulations associated with the protection of critical data and information assets in public and private sector institutions: Chapter 3 discusses the facilitating of electronic transactions; Chapter 5 deals with cryptography providers and stipulates the rules and regulations of cryptography providers; Chapter 8 of the ECT Act deals with the protection of personal information that is submitted and collected through the use of electronic transactions; Chapter 9 of the ECT Act deals with the protection of critical databases. In order to ensure that the government’s critical databases are adequately protected; Chapter 12 of the ECT Act stipulates the role and responsibilities of the appointment of a DG as a cyber inspector; and Chapter 13 of the ECT Act primarily deals with cybercrime in South Africa. This chapter is aimed at establishing and implementing mechanisms, tools, and strategies directed at cybercriminals and computer hackers.</td>
</tr>
<tr>
<td>Regulation of Interception of Communication and Provision of Information (RICA), No. 70 of 2002;</td>
<td>The RICA Act stipulates the regulations regarding the interception of communications and the processes thereof within the Republic. The Act further governs the interception or monitoring of both electronic and paper-based communications between institutions, systems and people internally and externally of government.</td>
</tr>
<tr>
<td>The Protection of Personal Information (PoPI) Act, No. 4 of 2013</td>
<td>The PoPI Act therefore ensures citizens’ constitutional right to privacy by ensuring that legislative policies are in place to protect personal information, as well as to ensure the regulation of the free flow and processing of personal information. The PoPI Act further stipulates the rights and privileges of citizens data and information from the unlawful collection, dissemination and use of personal in which the state must respect, protect and fulfill according to the Bill of Rights. The PoPI Act stipulates the (1) Conditions for lawful processing; (2) Cross-border transfers; and (3) Non-compliance with the Act.</td>
</tr>
<tr>
<td>Cybercrime and Cybersecurity Bill, No. 75 of 2015 (Department of Local Government and Human Settlements 2015:1);</td>
<td>The primary goal and purpose of the Cybercrimes and Cybersecurity Bill are to actively implement measures that will allow the establishment and implementation of penalties for persons or groups who are actively involved in committing cybercrimes in South Africa. The following chapters are dedicated to the regulation of cybercrime and cybercriminal behaviour: Chapter 2 of the Cybercrime and Cybersecurity Bill deals with the “powers to investigate, search and access or seize, and international cooperation; Chapter 6 of the Cybercrime and Cybersecurity Bill deals with the “Structures to Deal with Cyber Security” in South Africa; and Chapter 9 also stipulates that cross-border transfers of personal data and information.</td>
</tr>
</tbody>
</table>

Conclusions
One of the major challenges that was identified with the use of advanced technologies in public sector institutions is the heightened increase of cybercrime and cybercriminal activities. Cybercriminals in the 21st century have been consistently targeting their efforts at compromising public sector security systems and programs in order to gain unauthorised access to critical PSDI assets. Governments in developing and emerging economies are often affected and impacted the most due to their lack of advanced knowledge, skills, experience and expertise in cybercrime and cybersecurity strategies and approaches, as such as those in developed countries. Furthermore, another challenge is the lack of efficient and effective policies for cybercrime, such as the delayed implementation of the Cybercrimes and Cybersecurity Bill of 2015 in South Africa. Public sector institutions are particularly focused on the protection of their IT systems and infrastructure and lack effective DISG systems in order to improve the protection of their PSDI. The changing global environment triggered and driven by the 4IR through the introduction of new and advanced technological theories, processes, systems and practices requires the government to formulate and implement conducive policies, frameworks, laws, rules and regulations in order for the 4IR to successfully achieve, accommodate, and transition South Africa’s socioeconomic goals and objectives. Furthermore, the government should not only expect private sector institutions to be the leaders in 4IR research and development; it should take the initiative to establish public sector research hubs that will conduct and publish AI research material for the public sector. The formulation and implementation of integrated cybersecurity management, governance practices and approaches could assist the government in its efforts to counteract cybercrime, as well as ensuring its sustainable and long-term goals and objectives towards the achievement of effective cybersecurity practices and principles. In addition, this study was only conducted at a national sphere of government, hence further studies could be undertaken to identify, analysis and assess cybersecurity and threat intelligence practices in the provincial and local spheres of government. The policy and institutional contexts of the protection of PSDI assets play a critical role in the establishment and achievement of effective and sound DISG management policies, practices, systems, and standards in South Africa. The government has made tremendous strides by implementing policies, strategies, and frameworks that are aligned to the protection of its PSDI assets. The government has proved its willingness to abide by international best practices; a primary example is the PoPI Act of 2013, which was influenced by the Council of Europe Convention, the EU’s Data Protection Directive, and the OECD’s guidelines. This indicates that the government in general has the right types of policies in place for efforts geared towards DISG management practices; however, it is often challenged in the areas of implementation, compliance, monitoring, and evaluating of its policies. The security landscape of IT on both a local and international scale is constantly evolving and changes daily. This requires consistent efforts to keep up with best practices to adequately protect PSDI assets and to minimise the risks associated with the theft, misuse, unauthorised access, and fraudulent activities associated with cybercrime. The government must therefore implement proactive measures and approaches towards the protection of PSDI through effective DISG management practices that have a high focus on DISG risk management policies, strategies, models, and frameworks for the adequate identification and mitigation of internal and external risks that could significantly hamper the protection of PSDI.

Acknowledgement
This article is partly based on a published master’s dissertation, ‘Data and Information Security Governance in the Departments of Energy, Science and Technology, and Environmental Affairs’, by Lucia Masilela, under the supervision of Prof. Danielle Nel-Sanders, at the University of Johannesburg.

Author Contributions: Conceptualization, Methodology, Data Collection, Formal Analysis, Writing—Original Draft Preparation, Writing—Review And Editing by authors with equal participation. All authors have read and agreed to the published the final version of the manuscript.

Institutional Review Board Statement: Ethical review and approval were waived for this study, due to that the research does not deal with vulnerable groups or sensitive issues.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

Conflicts of Interest: The authors declare no conflict of interest.

References


Publisher’s Note: SSBFNET stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

© 2023 by the authors. Licensee SSBFNET, Istanbul, Turkey. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).