27th Annual INCOSE International Symposium (IS 2017)
Adelaide, Australia, July 15-20, 2017

Environmental Asset Management:

Risk Management Systems

Brian Naudé
Council for Scientific and Industrial Research
PO Box 395
Pretoria
0001
South Africa
+2712 841 2327
bnaude@csir.co.za

Charl Petzer
Council for Scientific and Industrial Research
PO Box 395
Pretoria
0001
South Africa
+2712 841 4292
CPetzer1@csir.co.za

Abstract. Environmental Asset Management (EAM) includes Environmental Asset Protection (EAP). Rare, important, and valuable natural assets need protection from vandalism and criminal syndicates determined to exploit these assets, for commercial gain or other purposes until the assets are exhausted. This paper addresses elements of environmental crime and the risk management strategies as part of EAP, including risk management system functions. A unique implemented risk management system in the Kruger National Park (KNP) is presented. Aspects of implementation are discussed including; challenges, lessons learnt, and initial measurable effects obtained.

Environmental Asset Protection Perspective

Environmental asset protection is one of several important environmental asset management functions. In this context, asset protection entails the protection of naturally occurring eco-systems that have complex and often unknown behavioural characteristics that vary over time, given interactions with other systems. In this context, naturally occurring eco-systems occur in oceans, inter-tidal zones and landwards environments that sustain various indigenous life forms. The interaction with human society as a system, arguably presents the highest risk to natural eco-systems that could lead to severe damage or overall destruction of these systems, including those under legal protection by human society. Environmental asset protection focuses on sustaining the diversity of an eco-system (conservation) and intensive protection (preservation) of identified highly threatened environmental assets. The methods used to effect conservation and preservation, are beyond the scope of this paper.

Elements of Environmental Crime

Causal Factors

The causal factors of environmental crime are inherent to human society and are mainly the following:

Cultural: Status perceptions and deep-rooted cultural beliefs associated with owning or consuming specific environmental artefacts or elements. There are two distinct markets. The status market dictates if the price goes up, the demand goes up. The "medicinal" market dictates if the price goes down the demand goes up. The normal rules of economics are not necessarily valid.

Societal: Poverty results in blatant theft of environmental assets to gain income by selling the stolen assets to a willing buyer irrespective of the legality thereof.

Habitat Loss: Encroachment of human settlements and harmful and/or illegal agricultural activity.

Factors Enabling Crime

Criminologists (LE. Cohen, M Felson, 1979) apply the Routine Activity Theory in order to argue that a crime can only occur when a likely offender, a suitable target and the absence of a capable guardian converges in time and space (Figure 1). Applying this theory, environmental crime can be disrupted by any one, or a combination of the following:

a. Reducing the likelihood of offenders, and/or preventing likely offenders from reaching suitable targets;
b. Reducing the availability and/or suitability of applicable targets, and
c. Ensuring that the guardian of the target is capable, and present.

An effective risk reduction strategy, *inter alia*, will address one, or more of these aspects to disrupt environmental crime.

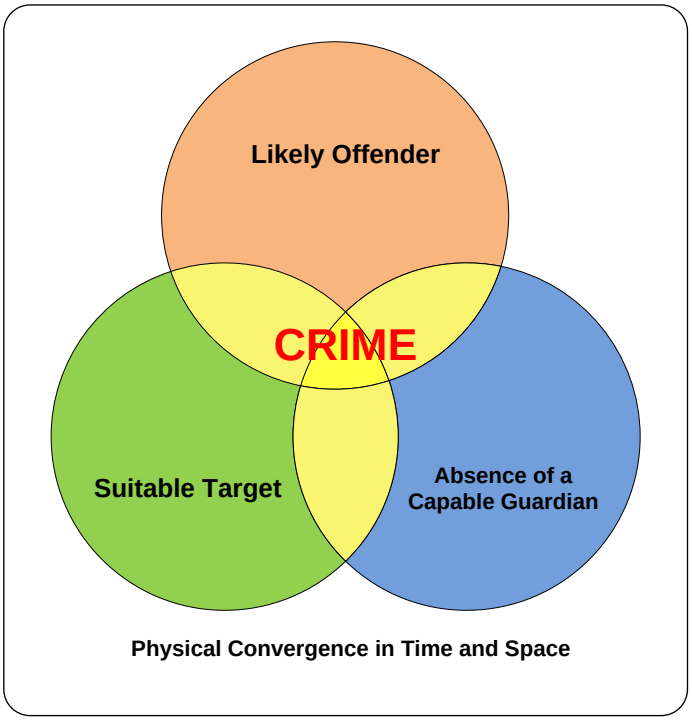

Figure 1: Routine Activity Theory

Environmental Asset Protection: Risk Management Strategies

Environmental asset protection includes the prevention and disruption of criminal activity. To this end, risk management strategies are required to give effect to the actions that reduce the risk of crime, as derived from the Routine Activity Theory mentioned above.

The risks that environmental assets face from criminal elements are compounded by the fact that criminal syndicates are well organised and funded and persistently adapt strategies to avoid prosecution. This implies that agile risk management strategies are required to disrupt criminal syndicate activity. In addition, the risk management strategies need to address certain causal factors stemming from cultural beliefs and poverty in the longer term. Furthermore, the trafficking of environmental assets has distinct markets, each with its own dynamics (UNDOC, 2016). Risk management strategies are required internationally, as stated by the Executive Director of UNDOC (Fedotov, 2013)

> "Wildlife and forest crime demands a global solution that offers international cooperation founded on joint operations, intelligence sharing and strong and compatible

national legislations. We can do nothing less. This is our shared planet; wildlife and forest crime is our shared responsibility".

The dynamics of the conflict, at various levels, between criminal and risk management systems is indicated in Figure 2.

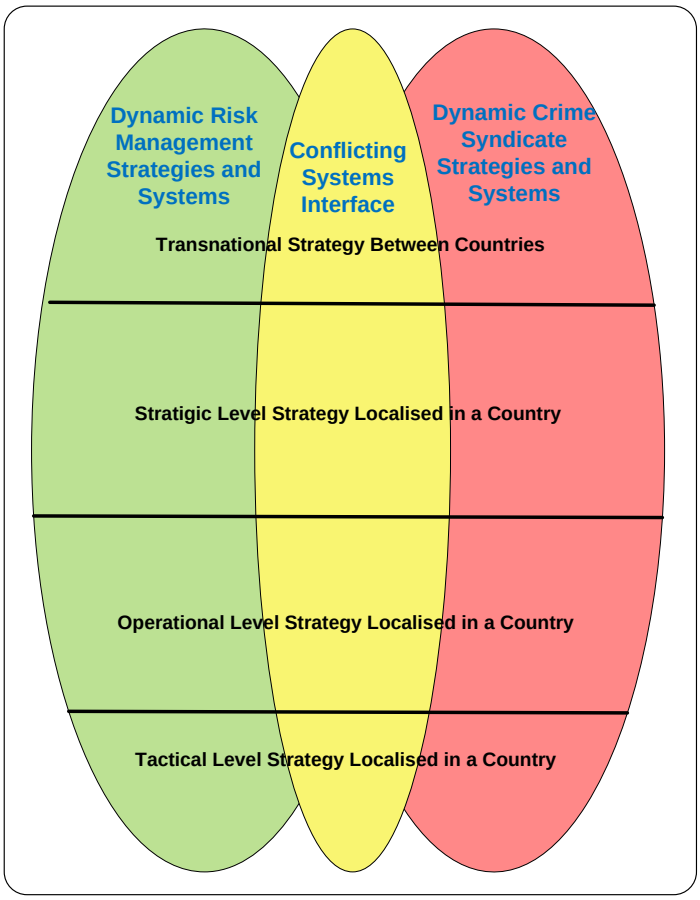

Figure 2: Conflicting Strategies and Systems

The key to risk management strategy is the definition of the measures of success. In a complex environment this invariably involves the use of a complex model that requires considerable data and analysis thereof, for sense making and decision support. The model, means for data collection and analysis thereof, needs to be designed into the particular risk management system.

Environmental Asset Protection: Risk Management Systems

Risk Management Functions

Risk management relies heavily on situation awareness, a cognitive state, and early warning of impending events within a specific time frame to enable pro-active counter measures to effectively place a competent guardian in a role to protect a target from a likely offender. Therefore, risk management systems need to perform certain functions to attain successful results. A functional framework that provides insight to the risk management processes and systems is provided in Figure 3. The timeline aspect is not shown because it varies considerably for given situations. The framework focuses on the risk management functions. The framework is used as an analysis tool to determine or assess the appropriateness of processes and enablers to perform the risk management functions given a specific objective.

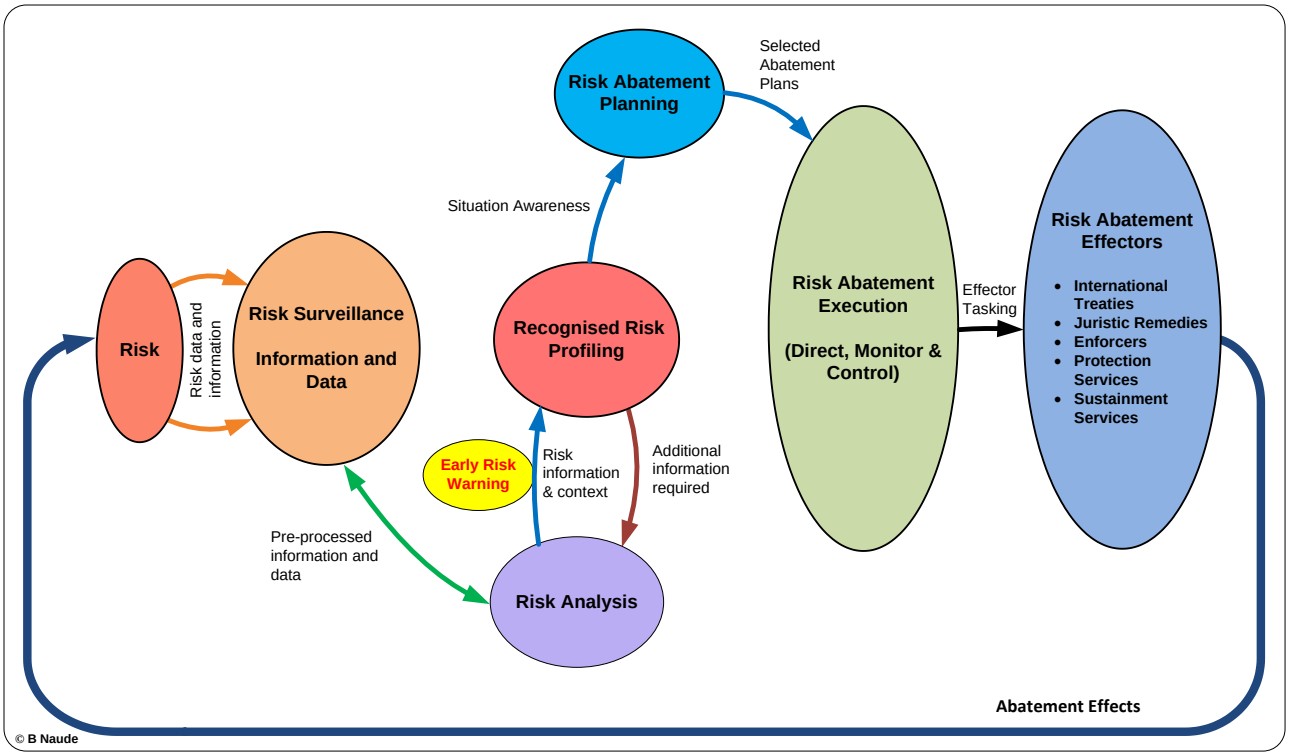

Figure 3: Risk Management Framework

A risk management system is required to enable the functions within the framework. The functions in the framework are described below. The framework is a specific variation of the generic one found in the ISO standard (ISO 31000-2009) as it incorporates aspects of command and control (DS Alberts, RE Hayes, 2006) and very specific functions related to Joint Intelligence-based Preparation of the Operational Environment (JIPOE) as contemplated in the publication (USA Joint Chiefs of Staff, 2009).

Concept of Situation Awareness: The concept of situation awareness, based on the aforementioned contextualisation, comprises a cognitive process unique to each individual and includes not only an awareness of facts and the context thereof for decision-making, but also an awareness of the consequences of decisions and the actions taken. This point is made as the term has many interpretations among individuals.

Risk: The risk is identified and characterised as more surveillance data and information is obtained by various sensors and placed in context to characterise risk for the purpose of obtaining early warning of a risk, amongst others.

Surveillance: Surveillance to obtain risk information can make use of technology, or humans or a combination thereof. Two types of surveillance are employed:

a. General surveillance to seek and identify risks;
b. Dedicated surveillance to characterise and track risks for neutralisation purposes.

The purpose of surveillance is to obtain data and information within a geographic and legal domain to identify and characterise (i.e. structure and behaviour) the risk. General surveillance focuses on obtaining data and information of all entities in a geographical domain for analysis. This type of surveillance is required in the entire geographical domain of interest. The data and information are utilised for the purposes of domain situation awareness synthesis. Dedicated surveillance focuses on obtaining data and information on specifically identified entities of interest in a geographical domain for analysis and action. This type of surveillance is done in the entire geographical domain of interest. The data and information are utilised for the purposes of creating specific entity risk profiles. The time value of the risk information may vary from very short to an extended duration.

Risk Analysis: Risk analysis contributes to situation awareness and comprises:

a. Making sense of all the data and information gathered;
b. Identifying information that is still required;
c. Assimilating the information and placing it in context to facilitate situation awareness within individuals and groups to obtain shared situation awareness and common focus.

This function requires that data and information must be retained for integrity and forensic purposes. The execution of this function requires several analysis tools and human independent systems that can provide alarms for early warning purposes when certain conditions are met. This function is often the most neglected one as it requires intense analysis effort and specific cognitive skills. The key output of this function is early warning information of a risk and relevant operational information required to compile recognised risk characterisation profiles.

Recognised Risk Profiling: The recognised risk profile contains information that has been filtered out of the domain awareness information to only show that which is relevant to:

a. Early warning of new risks;
b. Current risks (red force tracking);
c. Expected future risks;
d. Severity of risk consequences;
e. Status of current operations (monitoring actions, blue force tracking);
f. Planned operations;
g. New situations that need attention;
h. Other information relevant to inform decision-making relevant to operations;
i. Situation reports;
j. Incident reports, and
k. Asset locations if available and desired.

Risk Abatement Planning: Risk abatement planning includes pro-active preparation of the risk operations environment and planning of risk abatement operations based on long term objectives. It focuses on processes and resources required to execute operations in the designated geographical and legal domain. Tactical operations are planned to support operational level objectives in an integrated manner. Risk information plays a crucial role in this function.

Risk Abatement Execution: This function comprises risk abatement operations management, tasking relevant resources to execute tactical and routine operations as planned. Execution of tasked risk abatement action is monitored and corrective action implemented as required. Debriefing is performed and post action reports compiled for legal purposes. The gleaning of information obtained during risk abatement action is done and passed on to the risk analysis function. In a multi-party context this function can be problematic owing to differing operating procedures. (Example: police vs customs)

Risk Abatement Effectors: The risk abatement effectors are the means by which risks are abated or neutralised. These typically comprise:

a. International treaties;
b. Juristic remedies;
c. Enforcers;
d. Protection services, and
e. Sustainment services.

Risk Management Enablers: The risk management enablers (See KNP case) primarily consist of:

a. Surveillance systems (processes, humans, and technology);
b. Risk analysis systems (forensic processes, data analysis, and modelling);
c. Risk profiling system (processes, modelling);
d. Risk abatement planning systems (processes, modelling);

e. Command and control system (processes, operational information);
f. Effector systems (processes, enforcers, equipment);
g. Extensive secure communication networks, and
h. Inherent information and cyber security capabilities.

System Design Considerations

System design to implement the risk management functions needs to take important aspects into account. These aspects relate to elements in the environment in which the system is to be inserted and operated, and cannot be neglected. The aspects include but are not limited to:

a. International and country specific legislation;
b. The characteristics and dynamics of the identified risk profiles;
c. The selected risk management strategy objectives;
d. The specific geography and climate in which the system must operate;
e. The available infrastructure in the area of interest;
f. The existing operational procedures and the integration/transformation to those required;
g. The human capital available, and
h. The interface to other systems.

It is important to note that no single technology is capable of solving the risk management problem of environmental crime, nor any other risk problem. There is no universal solution as each solution is context-dependent, despite circumstantial commonalities. Different technologies require integration into a single coherent risk management system to address the different requirements pertaining to the risk profile. Different concepts need to be considered as input to the design of a risk management system. The routine activity theory and layered risk management are examples of concepts to be considered.

The Real World: Kruger National Park

The Kruger National Park is a significant world conservation area owing to a high level of biodiversity. The KNP falls under the jurisdiction of South African National Parks (SANParks). See www.sanparks.org

Geographical Context

The KNP is located in the north eastern part of South Africa. See Figure 4 (Courtesy of SANParks).

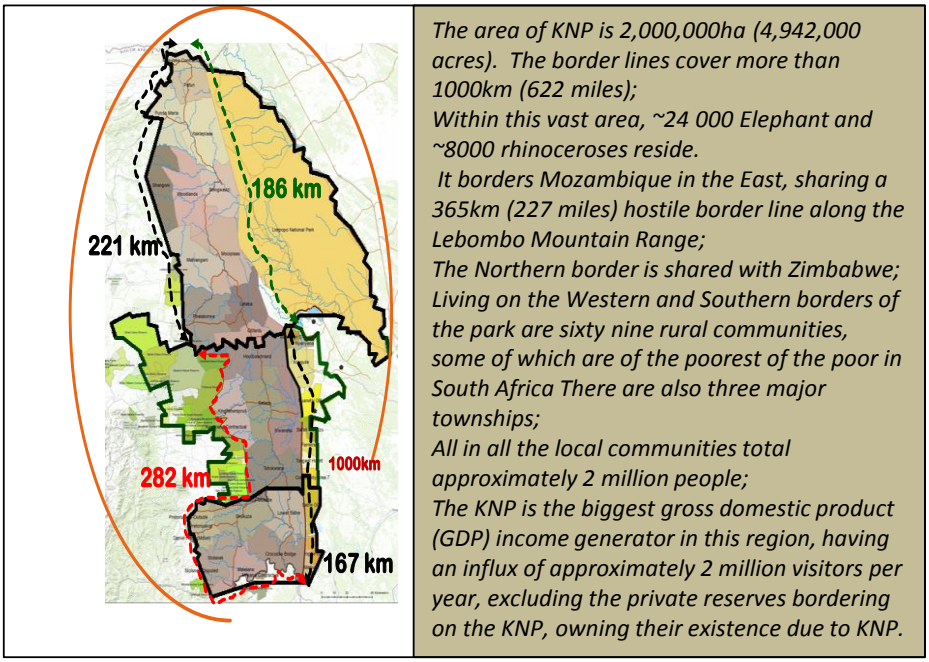

Figure 4: Kruger National Park Location and Map

The Environmental Asset Risk

The illegal removal of environmental assets from the KNP for reasons emanating from aforementioned causal factors constitutes a major risk for certain endangered species (CITES, 2016) that occur in the park. In particular the following are noted:

a. Black rhinoceros (*Diceros bicornis*);
b. White rhinoceros (*Ceratotherium simum*).

The key driver behind the risk appears to be international criminal syndication to satisfy the lucrative demand for wildlife products. This risk permeates all levels, i.e. local, national and international and constitutes loss of human life, biodiversity, and extinction of wildlife. Currently rhino horn is arguably the most expensive commodity in the world at an estimated US$60000/kg (WWF/Dalberg, 2012). South Africa has approximately 19700 rhinos, 80% of the world's population (R Bale, 2016). The white rhino population in the KNP constitutes the largest population in South Africa with between 8400 and 9300 under dire risk (E Molewa, 2016). The Figures 5, 6, and 7 (UNDOC, 2016) indicate the current trends with respect to the illegal trade in rhino horn. The trend indicates growing poaching with a possible decrease in the marginal rate during 2014-2015.

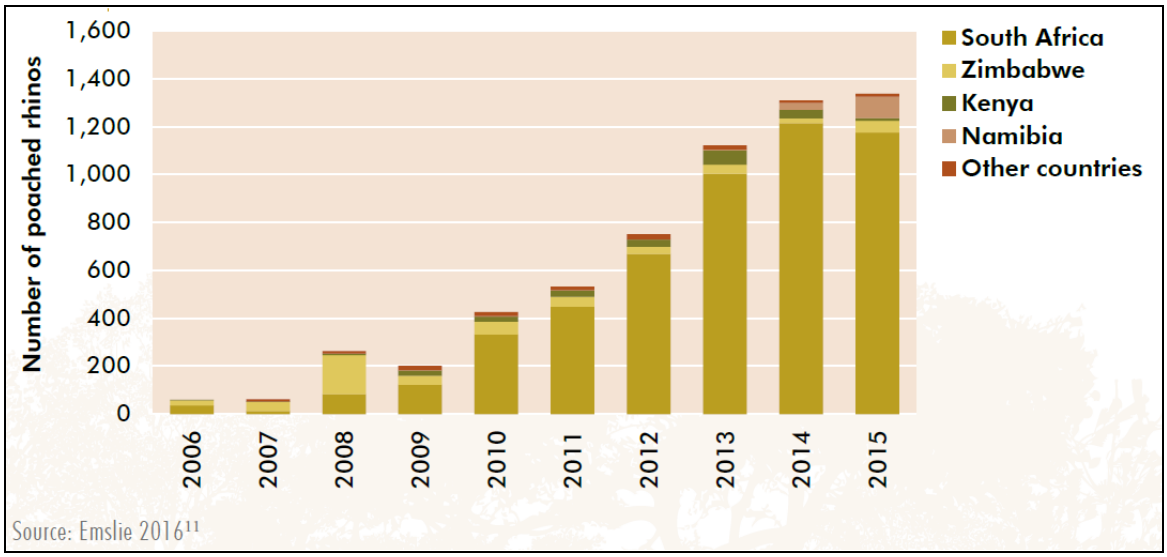

Figure 5: Number of Rhinos Poached by Selected Countries, 2006-2015

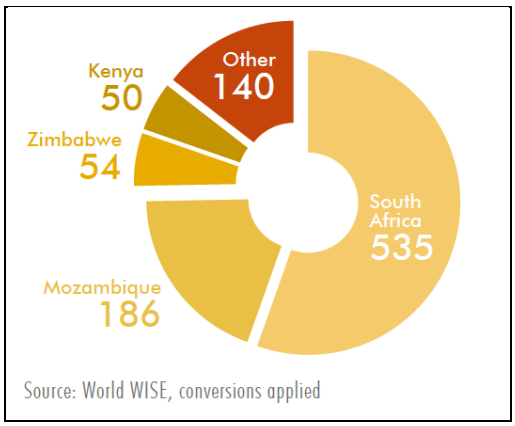

Figure 6: Share of Seized Rhino Horns (kg) by Country Identified as Source (Aggregated 2006-2015)

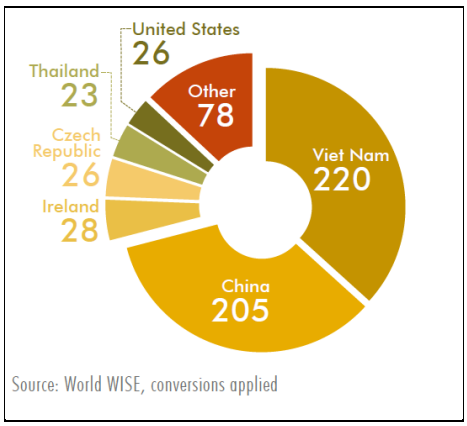

Figure 7: Share of Seized Rhino Horns (kg) by Country Identified as Destination (Aggregated 2006-2015)

The KNP Environmental Asset Risk Management Strategy

The risk management strategy[1] formulated for the KNP is to clear the KNP of poachers from the outside. This strategy is a layered protection approach involving strategies at all levels inclusive of other government departments and neighbouring organisations. The strategy involves dividing the KNP into three zones for operational reasons to integrate the efforts of neighbouring private reserves and transnational parks. The three zones are indicated in Figure 8 (Courtesy of SANParks).

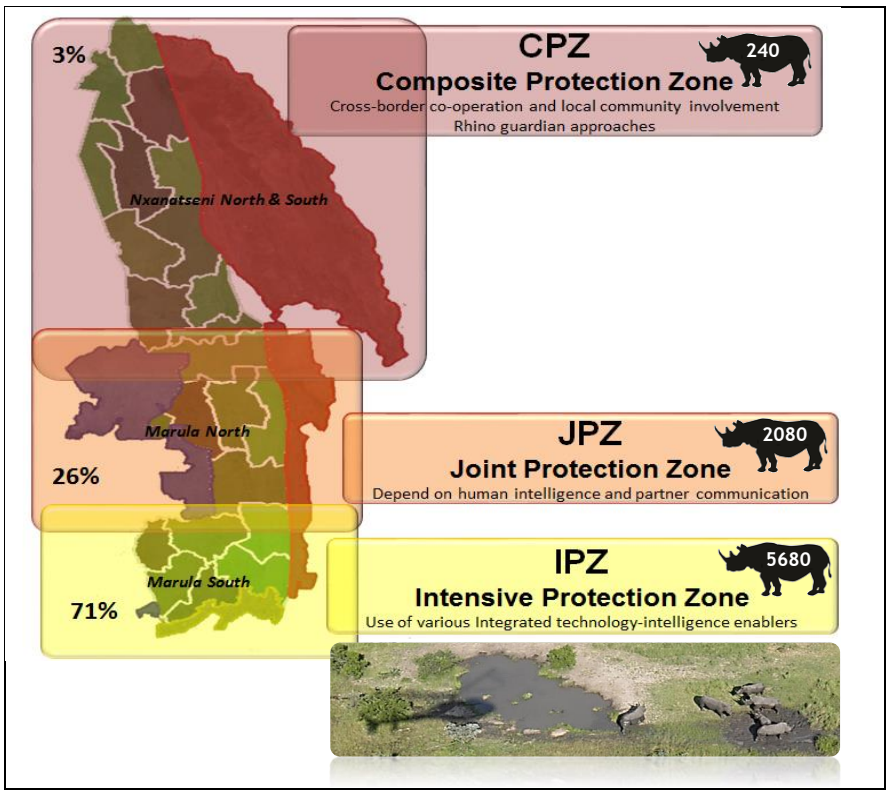

Figure 8: Operational Zones

Anti-poaching operations are based on risk information and are proactive and reactive in nature. The risk management strategy includes equipping the KNP officials with specific technological means to counter the risk within the KNP boundaries. Government departments are included within their respective mandates to take action in and outside the KNP to counter the risk. Formal interaction with neighbouring countries is established.

[1] Gen (ret) J Jooste (SANParks)

The KNP Environmental Asset Risk Management Enablers

The risk management functions as indicated in Figure 3 are implemented by means of the KNP Risk Management System which is operational. The KNP risk management system enablers utilise specific operating procedures and uniquely adapted technologies to form an integrated system of systems (See Figure 9) comprising:

Joint Operations Centre: All risk management activities are centered at a dedicated facility

Risk Information System: This system focuses on information on potential and known syndicates and perpetrators of environmental crimes.

Sensor System: The sensor system consists of the following in combined configurations:

a. Humans;
b. Canines;
c. Radars;
d. Electro-optics;
e. Standalone magnetic devices;
f. Linear magnetic devices;
g. Seismic devices, and
h. Data collection devices.

Risk Analysis and Profiling Systems: These systems consist of:

a. Humans;
b. Data bases;
c. Data reduction and analysis tools, and
d. Predictive modelling capability.

Planning, Operations, and Monitoring System. Operations planning, execution, and operations control take place on a modern integrated command and control system.

Effectors: Effectors consist of:

a. Armed rangers;
b. Canines;
c. Off road vehicles;
d. Air wing, and
e. SA Police and SANDF elements.

Communication System: Information and data exchanges between entities are facilitated by a broadband and tactical network.

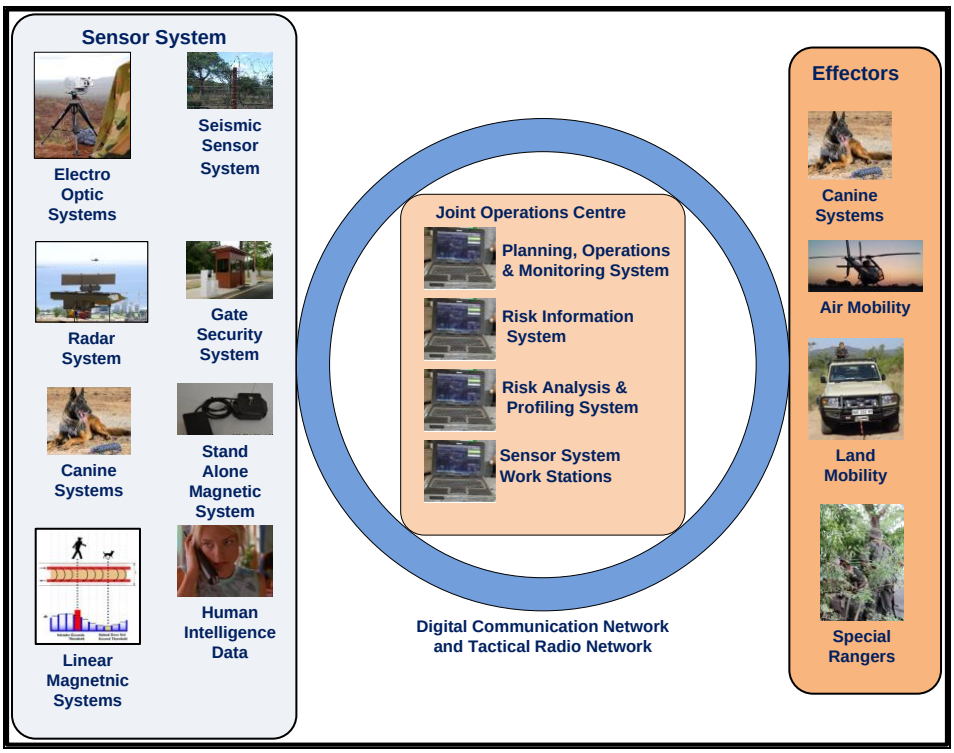

Figure 9: KNP Risk Management System of Systems

Challenges

KNP Internal Environment: The challenges in the KNP environment are many owing to the climate, nature of the terrain, and sheer vastness of the wilderness area, which hamper accessibility to all. Installed technology in this harsh environment is at risk owing to climatic conditions, susceptibility to damage by wildlife, theft, and sabotage. The successful detection of specific entities, amongst many types, in the KNP environment, required innovation to adapt technology for this purpose. Acceptance of new technologies from a personnel point of view, owing to the various levels of familiarity with technology, is also a challenge. However, this challenge is overcome with support and training.

KNP External Environment: The main challenge in the external KNP environment is the quick and drastic reduction in demand for wildlife products in the long term in the international domain. The large, relatively poor communities, with a high unemployment rate, living directly next to the KNP are in need of a source of income. This income is attainable through poaching owing to the local and high international demand for lucrative wildlife products.

Lessons Learnt

The following are some important lessons learnt by the role players during the implementation and operation of the KNP Risk Management System.

a. Inserting advanced technology into an environment that is technologically less mature presents its own unique problems in terms of acceptance of the new technology. Users are reluctant to use the capability enabled by the technology. More training and orientation is required to reduce the risk of non-use of the technology, which could result in function failure.
b. Physically installing advanced technology into the harsh environment such as that of the KNP has unique problems that are only exposed on site. Orientation of suppliers is provided, yet, and in spite of this a first time learning curve is experienced. This risk is usually short-lived. Proof of concept tests are done but are not always successful as extended test periods are required to reveal the flaws in a proposed solution. In some cases, such tests were conducted, resulting in risk reduction and rejection of the proposed solution. The risks emanate from extreme climatic conditions and the presence of dangerous wildlife.

c. Adapting sensors to distinguish between humans and wildlife is particularly difficult and more advanced techniques are required in the use of various sensors in logical configurations. This aspect was crucial in the selection of technology and was driven by risk reduction. The net result was application of a particular technology that is proving to be very successful.
d. Underestimating the logistics of operating in a vast wilderness environment. The wilderness area is characterised by insufficient infrastructure, bad or no roads, and dangerous aggressive free roaming animals. In many cases equipment and personnel need to be airlifted to reach certain sites. These factors introduce potential risks of schedule delays which need to be factored in.
e. Vendors of equipment need to understand the issues pertaining to the operational environment to add value to the risk reduction effort. Many vendors need to be oriented from a systems view to what is required and why. This stems mainly from the fact that they are not systems orientated and focus on the technology *per se*. This risk is managed by invitation to demonstrate the technology contribution to a specific operational activity in the selected environment. This is a successful strategy as in many cases the reality of the situation is experienced which results in a review of a solution proposal.
f. Underestimating the environmental protection governance issues applicable to a proclaimed national park. Any activities whatsoever that result in the disturbance of pristine wilderness areas, or modification of an existing disturbed area is subject to an environmental impact study by law. The insertion of technology is not a matter of fact and solutions proposed run a considerable risk of being rejected for environment protection reasons.

Initial Measurable Effects in the KNP

The measurable performance of the KNP Risk Management System implemented is provided in this paragraph (Information supplied courtesy of SANParks). The success of the interventions implemented is obvious from Figures 10 to 13 below which indicate annual data from 2012 to 2016. The current risk management system became operational during 2015. In Figure 10 the trend of poacher activity is compared to the number of rhino poached. The poaching activity, as can be seen, has increased significantly while the number of rhino poached has been stabilised with a negative marginal trend in 2016. The marginal year on year rates are indicated in Table 1.

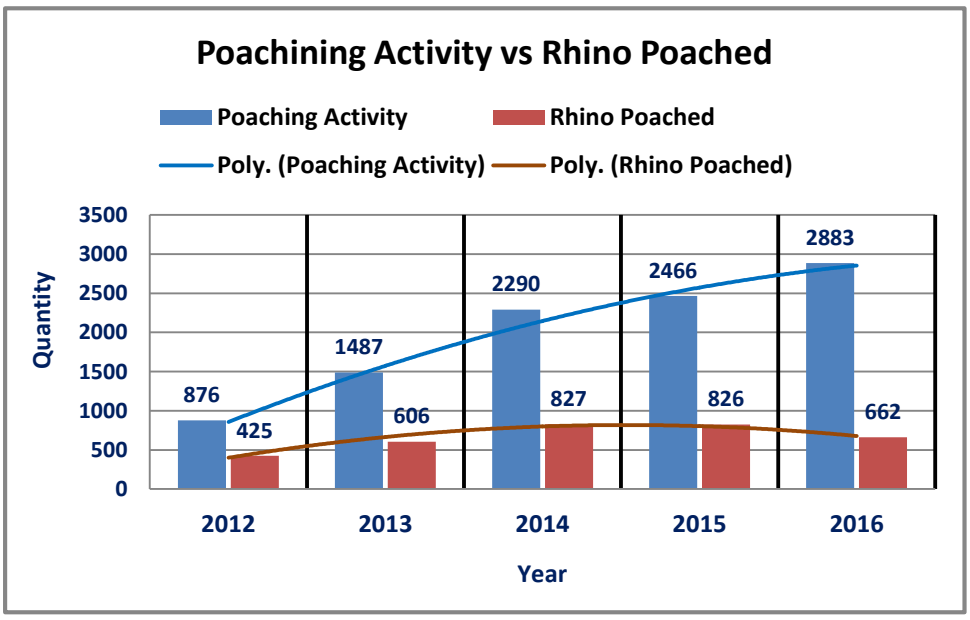

Figure 10: Carcasses and Poaching Activity (2012 to 2016)

Table 1: Marginal Rates Year on Year (Base year-2012)

Year	Poaching Activity % YoY	Rhinos Poached % YoY
2013	69.75%	42.59%
2014	54.00%	36.47%
2015	7.69%	-0.12%
2016	16.91%	-19.85%

Similarly, the number of poachers arrested (8.43/100 poaching activities) and fire arms confiscated (4.89/100 poaching activities) has increased consistently with the increase in poaching activity. This implies increased efficiency of the risk management system given the increase in poaching activity. The data for poachers arrested and firearms confiscated is indicated in Figure 11.

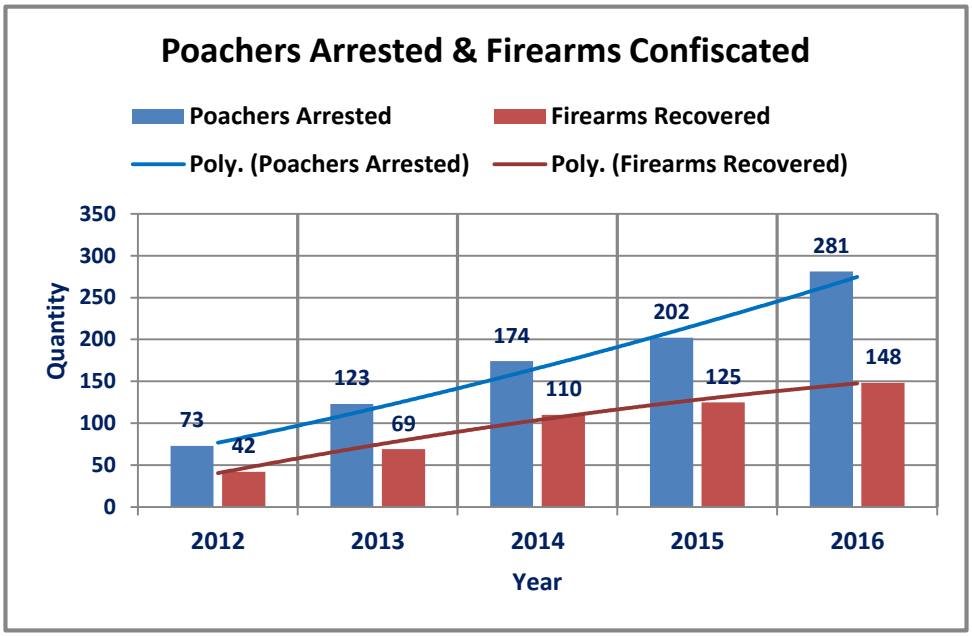

Figure 11: Poachers Arrested and Firearms Confiscated (2012 to 2016)

Figure 12 provides an overview of the KNP risk management effects and trends on poaching activity which are positive. Figure 13 indicates the trend of rhino poached per 100 poaching activities.

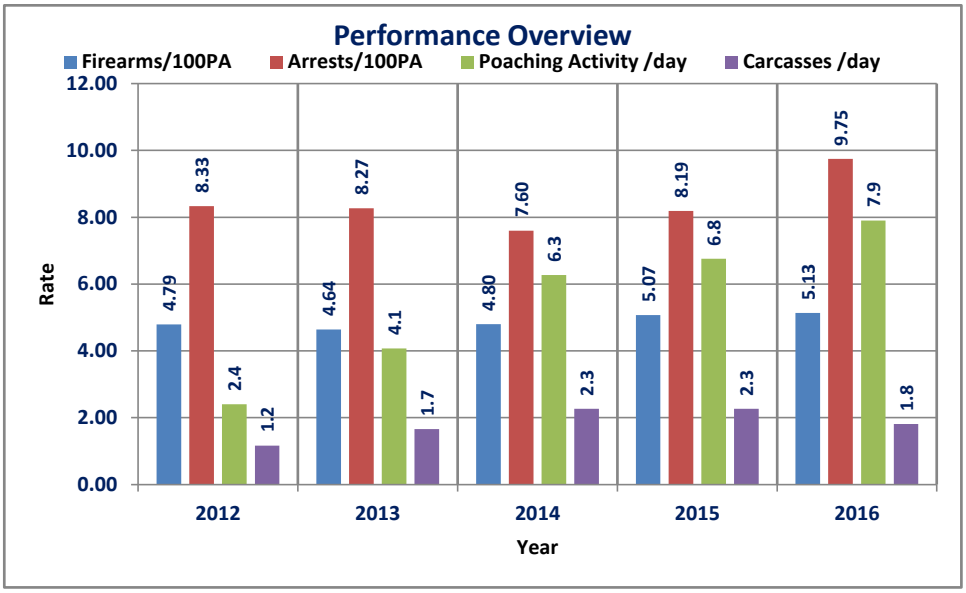

Figure 12: Rhinos Poached versus Poacher Activity (2012 to 2016)

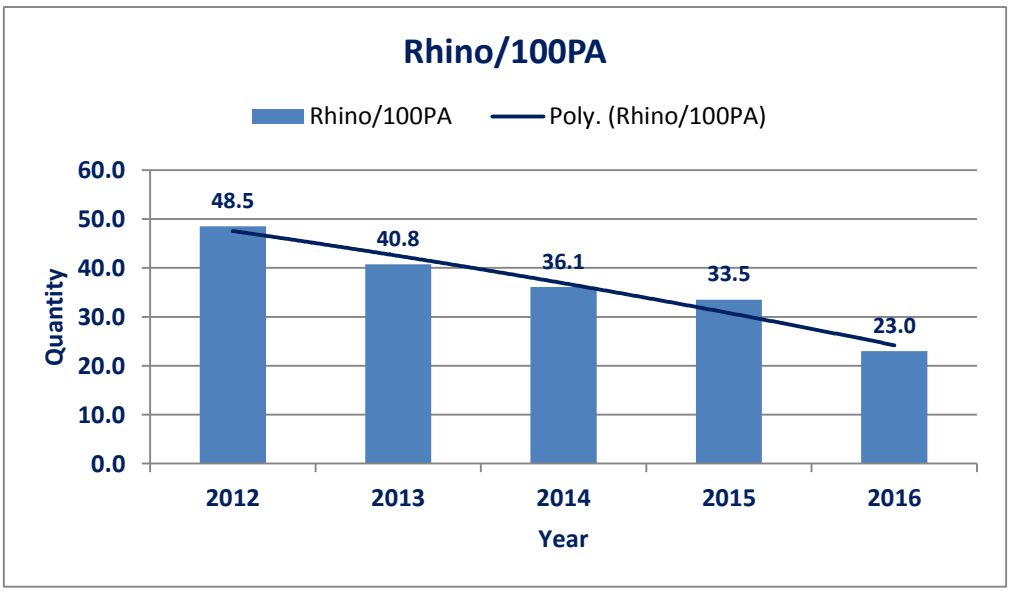

Figure 13: Rhinos Poached per 100 Poaching Activities

Concluding Remarks

The concluding remarks focus on the success or not, of the environmental asset risk management systems implemented internationally and locally in South Africa. The discussion is in context of international and KNP data presented on rhino horn trafficking.

International Risk Management System: The data presented on the quantity (kg) of rhino horn intercepted indicate that the international risk management system, implemented by nations, through CITES, is failing dismally, for various reasons. In the period 2006 to 2015 approximately 5085 rhino where poached in South Africa alone, this translates to 20,34 metric tons (based on an average 4kg per horn). For the same period only 1571kg (all sources) of rhino horn was reportedly intercepted at various ports in the world. Where are the other 18769kgs? Seemingly, mostly in China and Vietnam. The estimated value, at the current price, of stolen rhino horn for the mentioned period, is US$1460m. The main reason for the international risk management system failure has been identified (WWF/Dalberg, 2012) as the lack of will and law enforcement in the main source and destination countries. This system failure stems from failure in executing the **risk profiling, risk abatement planning,** and **risk abatement action** functions**,** at international level, within the risk management framework. Therefore, an alternative or modified international risk management strategy, based on accepted system architecture, is required to overcome blatant complacency within the international environment.

Prohibition: The strategy of prohibition on an activity is not just unsuccessful, but is futile and naïve, as no evidence of a successful prohibition strategy has yet been found. Crime syndicates thrive on prohibition which implies alternative effective strategies are required to reduce or eradicate the demand for wildlife products. Risk abatement measures *per se* will not change cultural beliefs, and other educational action in the destination countries is required to eradicate demand.

KNP Risk Management System: The KNP risk management system has been in operation in the IPZ for very short while, from 2015, and the data provided to date is indicative that the risk profiling, sensor systems, proactive abatement planning and anti-poaching operations are disrupting criminal activity (See Figures 10 to 12). The expansion of the system to other parts of the KNP is incomplete owing to fund constraints. This expansion is essential to further successfully disrupt criminal activity which is starting to occur in the northern parts. The introduction of similar risk management systems to other important national parks or conservation areas under threat would be very beneficial to all.

References

L E Cohen, M Felson, 1979, American Sociological Review 'Social Change and Crime Rate Trends: A Routine Activity Approach', American Sociological Association http://www.jstor.org/stable/2094589.

UNDOC, 2016, 'World Wildlife Crime Report: Trafficking in Protected Species', ISBN 978-92-1-148288-1. United Nations Office on Drugs and Crime.

Fedotov, Yury, 2013, 'Opening Remarks at the Twenty-Second Session of the Commission on Crime Prevention and Criminal Justice, CCPC.

ISO 31000-2009, Risk Management - Principles and Guidelines, International Organization for Standardisation.

DS Alberts, RE Hayes, 2006, Understanding Command and Control, ISBN 1-893723-17-8, DOD Command and Control Research Program (USA).

USA Joint Chiefs of Staff, 2009, Joint Intelligence Preparation of the Operational Environment, Joint Publication 2-01.3.

CITES, 2016, Appendices I, II, III, Convention on International Trade in Endangered Species of Wild Fauna and Flora.

WWF/Dalberg, 2012, 'Fighting illicit wildlife trafficking: A consultation with governments' WWF International, Gland Switzerland.

R Bale, 2016, 'Rhino Poaching Numbers Fall in South Africa in 2015' Wildlife Watch, National Geographic from http://news.nationalgeographic.com/.

E Molewa, 2016, 'Media release: Minister Edna Molewa highlights progress in the fight against rhino poaching' Dept. Environmental Affairs (RSA) from www.environment.gov.za/mediarelease.

Acknowledgements

SANParks for providing information related to the anti-poaching measures implemented in the Kruger National Park and the initial results obtained.

Biography

Brian Naudé is registered professional engineer with 35 years of project management and system engineering experience in military and other environments. He has been the lead system engineer on several large projects, the latest being the risk management system for the IPZ area of the Kruger National Park in South Africa. He holds a BSc Engineering degree from the University of Pretoria.

Charl Petzer is registered professional engineer with 30 years of programme/project management as well as systems engineering experience in military and other environments. He has been the lead systems engineer, as well as programme manager on several large projects/programmes, the latest being the Programme Manager for Environmental Asset Management Programmes at the CSIR, including for the IPZ area of the Kruger National Park in South Africa. He holds a Master's degree in Engineering, from the University of Pretoria.