Systemic approaches to critical infrastructure risk and security capabilities

Dr Duarte Gonçalves
CSIR
dgoncalv@csir.co.za

Chris Serfontein
CSIR
cserfontein@csir.co.za

Abstract. This article examines current and emerging threats to infrastructure as South Africa transitions from the National Key Points Act (NKPA), Act No. 102 of 1980 to the Critical Infrastructure Protection Act (CIPA), Act No. 8 of 2019. The aim is to provide risk and security architecture frameworks that will inform regulations and the design of security measures. To do this, the notion of risk and risk appetite are used to define the critical infrastructure risk model in terms of output risk; enterprise risk; input risk and threat risk. These risks are interpreted in relation to CIPA and its regulations. Threat risk is explored in more detail as a design basis for a security operational concept. Important areas that CIPA will need to augment will be contextualising critical infrastructure and essential infrastructure within an infrastructure ecosystem with a related strategy. In the last part of the article, the link between how the security operational concept address the threat risks and the constituents of a security architecture.

Introduction

While the nation state has made progress in creating goods and distributing these, it has also succeeded in distributing "bads", in what is known as the risk society (Beck, 1992). This article looks at current and emerging threats to infrastructure as South Africa transitions from the National Key Points Act (NKPA), Act No. 102 of 1980 to the Critical Infrastructure Protection Act (CIPA), Act No. 8 of 2019. In this context, this article aims to provide risk and security architecture frameworks that will inform regulations and the design of security measures. From a system engineering perspective it complements ISO 15288 while providing tailoring for critical infrastructure security.

Current and emerging threats in South Africa

New risks relating to infrastructure in South Africa are emerging beyond vandalism, theft, and organised crime. Three emerging categories of threats are orchestrated and synchronised hybrid threats, non-traditional security threats as well as threats that involve convergence of perpetrator and victim. Several examples are used to set the scene and are provided as motivation – they are historical and are the basis for a framework.

There is a possibility of terrorism[1] (seditious and treasonous acts) in SA leading to ideological destruction of infrastructure arising from two different sources. The first is related to the insurgency in Mozambique (DefenceWeb, 2021). While there are concerns that the Al Sunnah wa Jama'ah threat could spill over to South Africa, the more likely risk is the displacement of Mozambiquans into southern Africa (DefenceWeb, 2021). The second traces at least as far back as the July 2021 unrest. In the early hours of the 8th of July 2021 former President Jacob Zuma was incarcerated for contempt

[1] "terrorist activity" is defined in Section 1 of the *Protection of Constitutional Democracy Against Terrorist and Related Activities,* Act 33 of 2004 and spans 1.5 pages.

of court to serve a 15-month term handed down by the Constitutional Court. What started as a protest to free Zuma from prison quickly escalated to looting and violence (Hunter, Singh, & Wicks, 2021). These were coordinated incidents with an opportunistic component. Over 200 malls were ransacked and destroyed, factories and business were burned to the ground. More than 300 people lost their lives in the stampedes and ensuing chaos. What may constitute terrorism in law may not be considered so politically. The July 2021 unrest further highlighted supply chain risks nationally. Such supply chain problems are manifesting globally in part because of COVID and related production disruptions.

The Colonial Pipeline cyber-attack is an information security example where a hacker group called DarkSide received $90 million in Bitcoin ransom payments (Browne, 2021). The pipeline is a critical part of U.S. petroleum infrastructure, transporting around 2.5 million barrels per day of gasoline, diesel fuel, heating oil and jet fuel. The pipeline encompasses more than 8850 km and carries nearly half of the U.S. East Coast's fuel supply. DarkSide operates a "ransomware as a service" where they develop and market ransomware tools and sell them to other criminals who carry out attacks. The cyber-attack stopped pipeline operation and caused fuel shortages for days.

The ashes of the South African Parliament, a National Key Point, are still smouldering in a fire that started hours into 2022. Preliminary assessments reveal a lapse in monitoring of parliamentary surveillance footage where a suspect was caught on camera as early as 2 a.m. without any alarms being raised (News24, 2022).

Hybrid threats or methods of warfare (i.e. propaganda, deception, sabotage, etc.) have long been used by state and non-state actors to destabilise nation states, adversaries and undermine societies. This worldwide phenomenon has however in recent years picked-up in speed, scale, and intensity, facilitated by rapid technological development and global interconnectivity (NATO, 2021).

In South Africa over the past few years the hybrid methods became a mixture of coercive and subversive activities used by actors to exploit the vulnerabilities of the state or multi-lateral organs to their own advantage, while remaining under the threshold of warfare (Zandee, van der Meer, & Stoetman, 2021). These actors utilise a coordinated and synchronised mixture of measures (i.e. political, criminal, economic, labour, social, technological, legal, information, etc.) to achieve their objectives (Giannopoulos, et al., 2021).

Climate change will lead to more extreme weather events: heat waves, droughts, rainstorms, *flooding, fires (e.g. UCT Library)* and sea level rise. These **non-traditional security threats** in combination with reduced funding in a post COVID world, a lack of maintenance, and a culture that does not focus on maintenance, will lead to disruption of infrastructure or catastrophic failure, with catastrophic economic and social consequences for South Africa.

Other non-traditional security threats are also emerging. Space infrastructure, although not immediately visible from earth, has become a critical part of our modern daily life providing communications, navigation, aviation and maritime safety and surveillance services. New high-tech businesses and emergency coordination are dependent on these services which have economic and safety implications. However, as more satellites are launched, the risk of collisions with other satellites and debris from previous launches increases. In August 2021 the Yunhai 1-02, a Chinese military satellite was hit by Object 48078, a small piece of space junk from a Zenit-2 rocket (Wall, 2021). The risk is not only the loss of a satellite and related services, but debris from the collision may lead to a cascading series of collisions in space referred to as the Kessler effect (Kessler & Cour-Palais, 1978). At a time when space activity is increasing across the globe, cascading collisions could hamper space operations and access.

Threats that involve the **convergence of perpetrator and victim** (Beck, 1992) include pollution and climate change, electricity theft. Pollution from private companies and the state results in weather phenomenon that impacts infrastructure through climate change, as one example. As Beck points out, the results of the risk are not localised to the geographic location of the risk (Beck, 1992). Electricity theft, apart from the legal issues surrounding it in South Africa (Mujuzi, 2020), denies funding for resources, infrastructure and maintenance required to produce electricity. Once the infrastructure collapses, the perpetrator (amongst others) become the victim. However, since the action and consequences are separated in time and space the perpetrator may not realise that this is "punishment" but may have repercussions for the state in the form of unrest, for example.

In addition, these local risks must be contextualized globally where they are compounded through a US-China and a US-Russian struggle for power, and a potential (US) financial crash of a magnitude not seen before.

It is important that South Africa develop proactive and preventive approaches and frameworks to counter hybrid and non-traditional security threats. This will require protection of critical infrastructure, protection of public health and food security, enhancing cyber security, targeting threat financing, and building resilience against radicalisation and violent extremism.

The Critical Infrastructure Protection Act

South Africa is in transition from the NKPA to CIPA in terms of sections 29 and 30 of CIPA. New regulations in terms of section 27 of CIPA are still being drafted. This section highlights several definitions from CIPA and its purpose that are important in the context of this paper. From section 1, the following definitions are relevant:

> ***"basic public service"*** *includes a service, whether provided by the public or private sector, relating to* **communication, energy, health, sanitation, transport and water**, *the interference with which may prejudice the livelihood, well-being, daily operations or economic activity of the public;*
> ***"critical infrastructure"*** *means any infrastructure which is declared as such in terms of section 20(1) and includes a critical infrastructure complex where required by the context;*

To assist the reader, the definition of critical infrastructure (CI) is traced through section *20(1)(a)(i)* to section 16:

> *(1) Infrastructure qualifies for declaration as critical infrastructure, if—*
> *(a) the functioning of such infrastructure is essential for the economy, national security, public safety and the continuous provision of basic public services; and*
> *(b) the loss, damage, disruption or immobilisation of such infrastructure may severely prejudice—*
> *(i) the functioning or stability of the Republic;*
> *(ii) the public interest with regard to safety and the maintenance of law and order; and*
> *(iii) national security.*
> ***"critical infrastructure complex"*** *means more than one critical infrastructure grouped together for practical or administrative reasons, which is determined as such in terms of section 20(1)(c);*
> ***"threat"*** *includes any action or omission of a criminal, terrorist or accidental nature which may potentially cause damage, harm or loss to critical infrastructure or interfere with the ability or availability of critical infrastructure to deliver basic public services, and may involve any natural hazard which is likely to increase the vulnerability of critical infrastructure to such action or omission.*

Section 2 of CIPA outlines the purpose of the Act:

> *(a) secure critical infrastructure against threats; [...]*
> *(c) ensure that objective criteria are developed for the identification, declaration and protection of critical infrastructure;*
> *(d) ensure public-private cooperation in the identification and protection of critical infrastructure;*
> *(e) secure critical infrastructure in the Republic by creating an environment in which public safety, public confidence and basic public services are promoted—*
> *(i) through the implementation of measures aimed at securing critical infrastructures; and*
> *(ii) by mitigating risks to critical infrastructures through assessment of vulnerabilities and the implementation of appropriate measures;*

Of specific interest to this article is section 20:

> *(1)(b) categorise critical infrastructure or certain parts of such critical infrastructure that is declared in terms of paragraph (a) in either a low-risk, medium-risk or high-risk category, as may be prescribed;*

This paper addresses the framework for how to define the risk needed to categorise the CI which formed the basis of inputs to CIPA regulations provided by the authors. Other parts of CIPA that are important for the purpose of this article will be quoted as required. For the rest of the Act, the reader is referred to CIPA.

Overview of the article

Systems approaches are used to place infrastructure within an enterprise, and an enterprise within an ecosystem. This article will discuss CI, an Infrastructure Ecosystem and different types of risk. Risk-based approaches have limitations in dealing with uncertainty and to address this, the concept of resilience is introduced. This first part of the article defines the framework of the security problem.

The importance of a reference security architecture is discussed as a bases for designing the security capability for a particular CI. The focus shifts to developing a security architecture starting with a process for developing a security architecture, the development of security operational concepts informed by the risk analysis, the elements of a security architecture and finally vertical and horizontal integration of the security architecture.

Critical Infrastructure, an Infrastructure Ecosystem and Risk

Section 19(1) (b) of CIPA requires categorising infrastructure risk as low-, medium- or high-risk considering the impact and consequence of failure, disruption or destruction of the infrastructure and the probability of such consequences. The Act does not elaborate on what risks must be considered for categorising infrastructure risk within the purpose of the CIPA (Section 2). To understand this, this section introduces the notion of risk and risk appetite, defines, and contextualises CI, essential infrastructure (EI) and the concept of an infrastructure ecosystem. Within this context, the CI risk model output risk, enterprise risk, input and threat risk are discussed. Lastly, these risk types are linked to CIPA and its regulations.

It should be noted that the risk model presented is somewhat linear and simplistic because the purpose of this article is to formulate an infrastructure risk framework and to communicate it rather than to provide theoretical explanation. To properly secure infrastructure given the complexity arising in an infrastructure ecosystem, risk frameworks must be extended to include uncertainty and resilience.

CI, EI and an infrastructure ecosystem

This section establishes the relationships between CI and EI. In terms of section 16 (1) of CIPA, repeated here for convenience:

> *"(1) Infrastructure qualifies for declaration as critical infrastructure, if—*
> *(a) the functioning of such infrastructure is essential for the economy, national security, public safety and the continuous provision of basic public services; and*
> *(b) the loss, damage, disruption or immobilisation of such infrastructure may severely prejudice—*
> *(i) the functioning or stability of the Republic;*
> *(ii) the public interest with regard to safety and the maintenance of law and order; and*
> *(iii) national security."*

The requirements in section 16(1), are subject to one or more of the following criteria from section 16(2) being applied:

> *"(a) the infrastructure must be of significant economic, public, social or strategic importance;*

> *(b) the Republic's ability to function, deliver basic public services or maintain law and order may be affected if a service rendered by the infrastructure is interrupted, or if the infrastructure is destroyed, disrupted, degraded or caused to fail;*
> *(c) interruption of a service rendered by the infrastructure, or the destruction, disruption, degradation, or failure of such infrastructure will have a significant effect on the environment, the health or safety of the public or any segment of the public, or any other infrastructure that may negatively affect the functions and functioning of the infrastructure in question;*
> *(d) there are reasonable grounds to believe that the declaration as critical infrastructure will not have a significantly negative effect on the interests of the public;*
> *(e) the declaration as critical infrastructure is in pursuance of an obligation under any binding international law or international instrument; and*
> *(f) any other criteria which may, from time to time, be determined by the Minister by notice in the Gazette, after consultation with the Critical Infrastructure Council."*

Note that while CIPA has a definition for CI in section 1, it defines CI in terms of the criteria for *declaring* infrastructure as CI. This leaves open (or implied) whether CI is the physical infrastructure or if CI includes the CI enterprise. This will be made explicit later in this section.

EI is defined in the *Criminal Matters Amendment Act (CMAA),* Act No. 18 of 2015 as:
"any installation, structure, facility or system, whether publicly or privately owned, the loss or damage of, or the tampering with, which may interfere with the provision or distribution of a basic service to the public".

The main difference between EI and CI is that EI is limited to the provision or distribution of a basic service. CI may be broader including significant economic, public, social or strategic importance. It also includes "*significant effect on the environment, the health or safety of the public or any segment of the public".* Importantly, infrastructure qualifies as CI if interruption of the infrastructure service will have a significant effect on "*any other infrastructure that may negatively affect the functions and functioning of the infrastructure in question".* This criterion acknowledges interdependence on other infrastructure. Other criteria relates to public interest, international obligations and determinations by the Minister of Police in consultation with the Critical Infrastructure Council.

Neither the CIPA nor the CMAA explicitly place the infrastructure within an enterprise responsible for its sustainable operation and maintenance. In this article we place EI or CI within an **EI or CI enterprise**. *When CI or EI is placed within the enterprise context, interdependencies between the infrastructure and operations, enterprise support and information security become apparent.* Furthermore, to make explicit the interdependence of infrastructure on other infrastructure (section 16(2)(c)), an **infrastructure ecosystem** is defined (Figure 1). Figure 2 illustrates sectoral interdependence. As an example, the generation of electricity is necessary for rail transport which in turn is necessary for the transport of coal used in the generation of electricity (Yusta, Correa, & Lacal-Arántegui, 2011). The infrastructure ecosystem exists within a regional and social context. But two other interdependencies must also be considered: the three-tiered structure of government in South Africa, namely national, provincial and local government and the distribution of CI geographically. Thus, the ecosystem level is the most complex and requires methods beyond just risk analysis.

Risk and a CI risk model

Risk is the mapping of the probability and the consequences of a hazard or threat (Haimes, 2009) as illustrated in Figure 3. What constitutes an acceptable level of risk depends on context. In a low risk appetite context, there would be more red blocks while in a high risk appetite context there would be more green blocks. The risk appetite is not defined in the Act but is relevant to the Regulations. The purposes of risk assessment in achieving CI security are:

- Categorisation – CIPA sections 19 and 20;
- Design (design basis threat);
- Assurance (Review of the process including validation); and

- Operations - threat risk assessment (intelligence) for tactical, operational and strategic use and investigations (counter-intelligence).

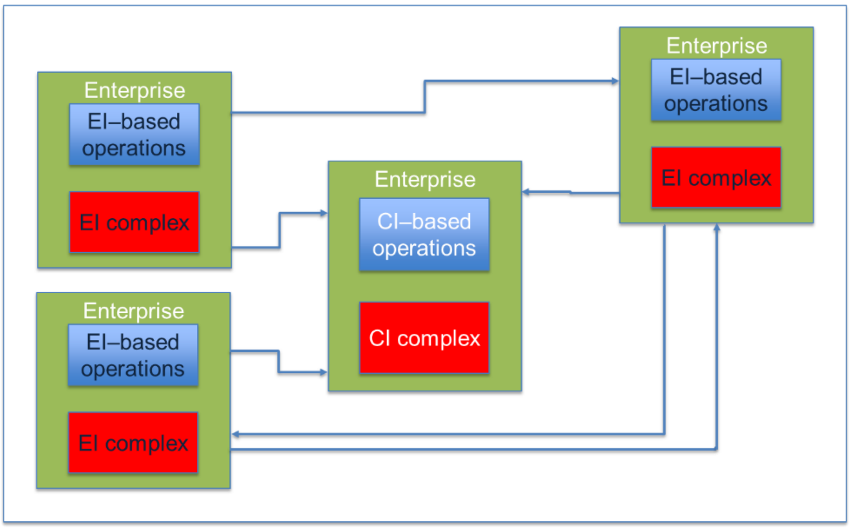


Figure 1 An infrastructure ecosystem

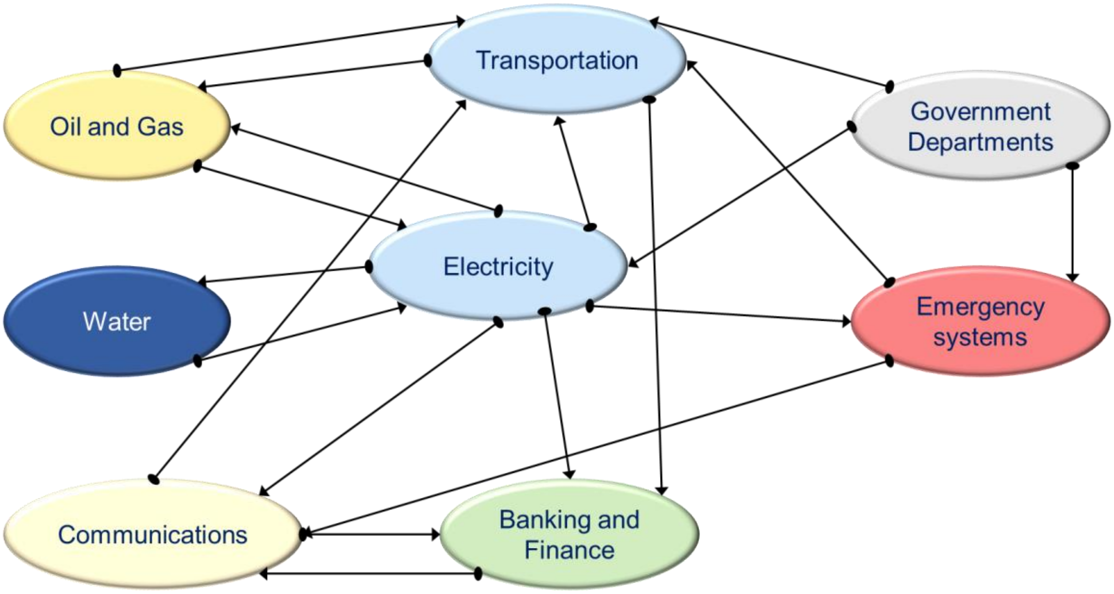


Figure 2. Example of CI interdependence

The purpose of the risk assessment determines the sources (stakeholders, subject matter experts, historical data and scanning) of information, the methodologies to be used and the risk time horizon that must be considered, e.g., a security investment is on a time horizon of five years. The stakeholders will have different perceptions about, and ability to take risk. A threat evaluation is sector-specific and certain sectors such as nuclear and aviation are governed by international bodies.

To create a CI risk model we start with a simple framework based on input, enterprise (internal) and output risks illustrated in Figure 4. The examples provided for each risk type are illustrative and may not be complete.

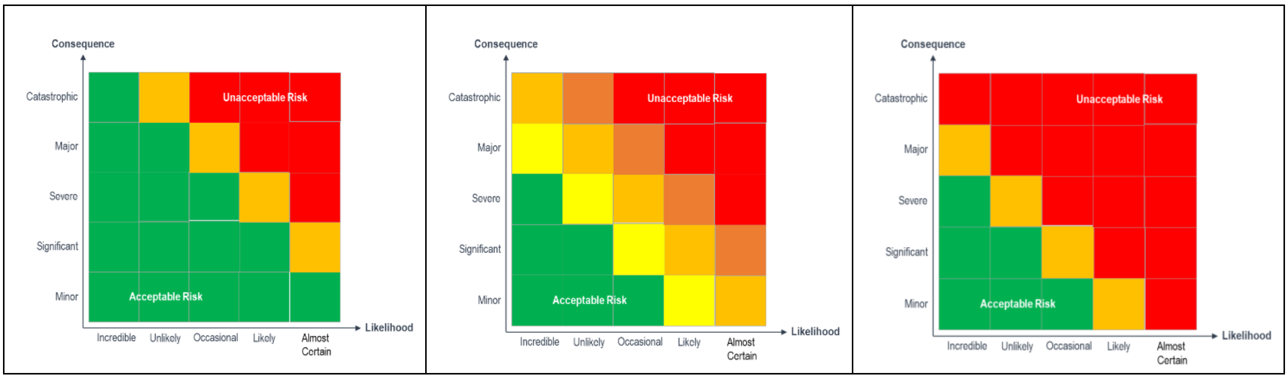


Figure 3. The concept of risk with decreasing risk appetite from left to right

Risk always impacts **effectiveness**. Measures of CI effectiveness can be availability (Up time / Total time), CI replacement time and cost which further develop the criteria of CIPA section 16(2). Other measures of effectiveness should be defined based on the specific type of CI, for example: Capacity (Power, volume rate, people per hour), System Average Interruption Duration Index (average duration of interruption in electrical power supply indicated in minutes per customer) or System Average Interruption Frequency Index (average frequency of interruptions in electrical power supply). Such measures can be evaluated geographically to provide additional diagnostic value.

Output risks arise from the CI not being available as contemplated in section 16(2)(a)-(d) of CIPA. The output risks are, broadly, national societal risks and output resource risks. The national societal risks include economic, political, social, environmental, safety and security risks. The output resource risks relate to the provision of basic public services depending on the specific type of CI and include for example: the disruption of energy, health, sanitation, transport, communication, or water services. Measurable output risk consequences include:

- Financial cost arising from repair of CI, or, in the worst case, replacement;
- The time required to rebuild the CI;
- Number of deaths arising from the CI or a lack of CI availability;
- Loss of quality of life arising from the CI or a lack of CI availability; and
- Opportunity cost arising from the CI or a lack of CI availability.

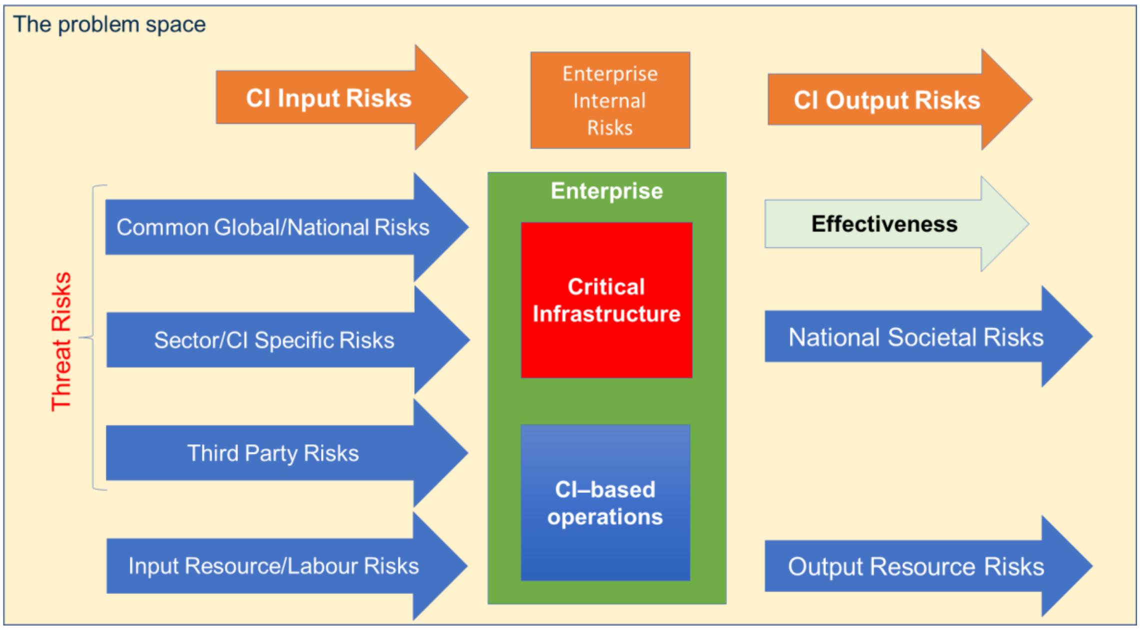


Figure 4 The CI risk model

The input risks include:

- Security risks arising from threats to CI (discussed further below and in the section Threat and Security Risk) and includes: Common global and national risks, sector or CI specific risks and third party risks;
- Resource risks relating to insufficient capital, knowledge, skills, technology, information, communication, energy, health, sanitation, transport and water, etc. required by the CI enterprise to ensure the availability of its services; and
- Labour (union or strike) related risk.

Common global and national risks affect all infrastructure within the ecosystem. Examples of such risks include:

- Political risks;
- Economic risks including a global financial crash;
- Legal/regulatory risks;
- International obligations;
- Military risks;
- Organised crime risks;
- Large scale social unrest; and
- Environmental risk of which global climate change is one.

Since these risks are common, they can be assessed by a small number of forums and organisations, for example, National Intelligence Co-ordinating Committee, State Security Agency, South African Police Service, and the South African National Defence Force, at a national level, for the benefit of the CI community on an ongoing basis.

Third-party risks arise from parties providing systems (including information systems) and services, such as guarding, to the CI enterprise and would likely have access to the CI infrastructure and information.

Enterprise risks relate to the strategic, operational and tactical management of the CI enterprise. Enterprise risks include governance and management failures, failure to manage risk, failure to develop and implement an enterprise strategy, failure to manage resources, lack of internal controls. Corruption is sometimes an enterprise level risk. However, in South Africa corruption is a systemic risk that impacts CI ecosystem, that it has been termed “state capture” (Zondo, 2022).

For each type of risk, different types of risk assessments are required. Table 1 lists the risk types and their significance in the context of CIPA. The security risk assessment is an input to the Security Policy and Plan (CIPA Section 24(7)(a)) the security capability design as well as the ability to respond to emergencies and implementation of contingency plans. A capability is the “ability to do something” at a level in a systems hierarchy that includes people. Once the policy and plan are in place, there may be a gap between the current security capability and the required capability. There may be enterprise risks in providing the required security capability which need to be assessed.

Table 1. CI risk types and their significance

Risk type	Significance in the context of CIPA
National societal risk	Categorisation of CI risk as per Sections 19(1) and 20(1) of CIPA
Output and input resource risk in conjunction with Common national and global risks	Development of a national infrastructure ecosystem strategy including emergency response and contingency plans at a national level with the provision of emergency resources for securing the ecosystem.
Threat risk	Input to the Security Policy/Plan, Security Operational Concept and capability design, emergency response and contingency plans. Assurance requires ongoing threat risk assessment.

	Operational risk assessment. Common national and global risks are ideally provided to CI community by relevant organisations but must be interpreted for the specific CI enterprise in the Security Policy/Plan.
Input Resource and Labour risks	The enterprise management must sustainably manage input resources, labour and the enterprise capabilities required for the services provided by the CI and its security. The security capability is implemented by the enterprise and subject to inspection by the Regulator against an approved Security Policy/Plan to assure quality.
Enterprise risk	
Third party risk	Requires a security process for assessing and managing third party risk.

Table 1 is primarily for CI enterprise level risks. At the ecosystem-level, the CIPA Regulator must develop systems for dealing with security and resource risks that are interdependencies between or affect multiple infrastructure whether CI or EI.

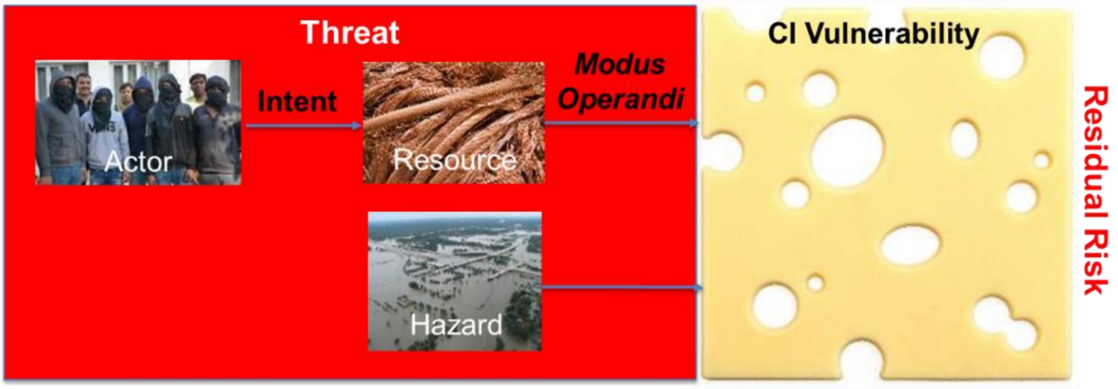
Threat and Security Risk

Threats as defined in section 1 of CIPA includes malicious activity as well as hazards. These threats may be specific to geographic regions, across the entire country, or the region and may even have global ramifications, such as (adapted from (CISA, 2019)):

- Climatological events (extreme temperatures, drought, wildfires);
- Hydrological events (floods);
- Meteorological events (tropical cyclones, severe convective storms, severe winter storms);
- Geophysical events (earthquakes, tsunamis, volcanic eruptions);
- Pandemics (global disease outbreaks);
- Space events (geomagnetic storms, satellite collisions);
- Technological and industrial accidents (structural failures, industrial fires, hazardous substance releases, chemical spills);
- Unscheduled disruptions (aging infrastructure, equipment malfunction, large scale power outages);
- Criminal incidents and terrorist attacks (vandalism, theft, property damage, environmental crime, active shooter incidents, kinetic attacks);
- Cyber incidents (denial-of-service attacks, malware, phishing);
- Supply chain attacks (exploiting vulnerabilities to cause system or network failure);
- Foreign influence operations (to spread misinformation or undermine democratic processes); and
- Untrusted investment (to potentially give foreign powers undue influence over SA critical infrastructure).

These threats and hazards must be identified, and their possible consequences on the infrastructure estimated. A framework for the assessment of threats, especially of a malicious nature, is provided in Figure 5. A malicious threat has an actor with a specific intent on a certain resource (Gonçalves, 2018). An actor includes an individual, a group, or a state. An actor may be engaged in malicious or illegal activity, organised criminal, or protests. The resource may range from people, fear, power, money, media attention, information, privileges, and race. The *modus operandi* considers how the actor will hide their identity; completes the crime successfully and escapes. In line with the CIPA's definition of threats, hazards are included such as natural events (floods and fires) and accidents. The CI may have vulnerabilities such as the absence of physical security measures; slow security response; poorly managed information security; or low staff morale. The residual risk is explained metaphorically using the Swiss cheese model. Threats that can penetrate various slices of cheese when the holes align, is the residual risk. *If the input risks are not sufficiently mitigated, the residual risk may result in output risks manifesting*.

The model of Figure 5 is greatly simplified. States may use non-state actors or other transnational actors to give form to their strategic objectives. Because South Africa faces hybrid threats, these risks occur in combinations. A conceptual model of hybrid threats is illustrated in Figure 6. Ultimately, CI is a collateral victim of action against the state.



l

Figure 5. CI Threat and vulnerability model

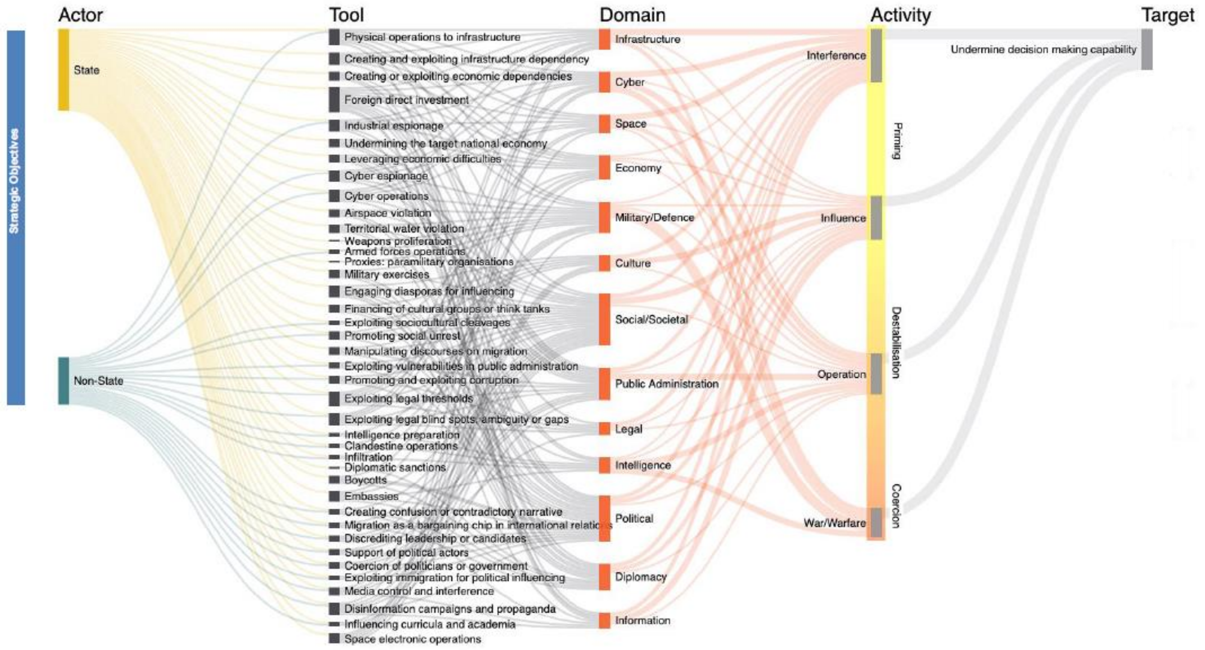

Actor
Tool
Domain
Activity
Target
Strategic Objectives
State
Non-State
Physical operations to infrastructure
Creating and exploiting infrastructure dependency
Creating or exploiting economic dependencies
Foreign direct investment
Industrial espionage
Undermining the target national economy
Leveraging economic difficulties
Cyber espionage
Cyber operations
Airspace violation
Territorial water violation
Weapons proliferation
Armed forces operations
Proxies: paramilitary organisations
Military exercises
Engaging diasporas for influencing
Financing of cultural groups or think tanks
Exploiting sociocultural cleavages
Promoting social unrest
Manipulating discourses on migration
Exploiting vulnerabilities in public administration
Promoting and exploiting corruption
Exploiting legal thresholds
Exploiting legal blind spots, ambiguity or gaps
Intelligence preparation
Clandestine operations
Infiltration
Diplomatic sanctions
Boycotts
Embassies
Creating confusion or contradictory narrative
Migration as a bargaining chip in international relations
Discrediting leadership or candidates
Support of political actors
Coercion of politicians or government
Exploiting immigration for political influencing
Media control and interference
Disinformation campaigns and propaganda
Influencing curricula and academia
Space electronic operations
Infrastructure
Cyber
Space
Economy
Military/Defence
Culture
Social/Societal
Public Administration
Legal
Intelligence
Political
Diplomacy
Information
Interference
Influence
Operation
War/Warfare
Priming
Destabilisation
Coercion
Undermine decision making capability

Figure 6. A conceptual model of hybrid threats (Giannopoulos, et al., 2021)

Risk, complexity, and resilience

In the case of risks, we are dealing with future events that can be imagined, where large numbers of historic observations may be available, and probabilities can be determined (Figure 7). In the case of uncertainty as an ontological characteristic of complexity, probabilities cannot be determined. Sometimes there are events that cannot be imagined, or the magnitude of their consequences are unimaginable. While risk management has its place, when faced with deep uncertainty or unknown unknowns, we may need additional concepts.

Having introduced hybrid and non-traditional security threats within the context of the infrastructure ecosystem, the complexity of the security problem is glaring. Resilience requires anticipating, avoiding, reconstructing, or otherwise minimising the effects and duration of a disruption caused by a threat or hazard (Hollnagel, Woods, & Leveson, 2006). Enterprise resilience is dependent on management, culture, and infrastructure not just technical factors. Resilience helps us address those scenarios that cannot be anticipated at planning time because of uncertainty and incomplete information.

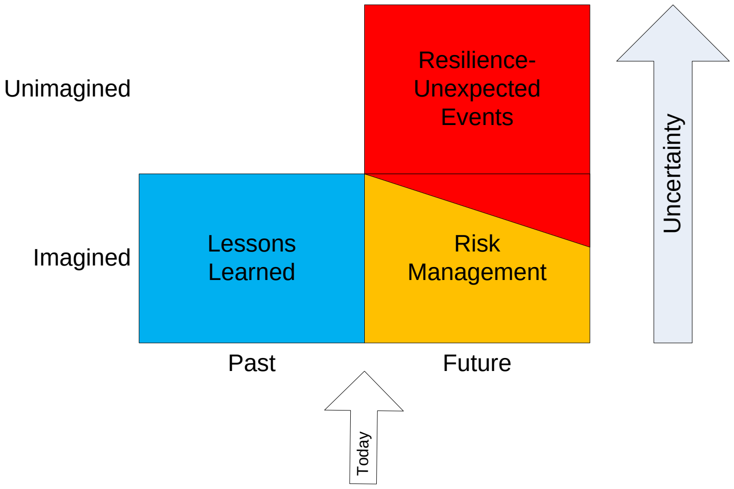


Figure 7. Moving beyond risk - uncertainty

CIPA's definition of ''resilience'' is "*the ability of infrastructure to mitigate, absorb or withstand any damage, disruption, disturbance or interference in order to maintain the functionality, integrity and structural capacity of that infrastructure*" (S1. CIPA, Act No. 8 of 2019). This resilience definition is in relation to infrastructure and not the enterprise within which the infrastructure resides. The definition in terms of "*any*[2] *damage, disruption, disturbance or interference*" will make the infrastructure expensive, impractical or impossible to retrofit if it is to be resilient in CIPA terms. Infrastructure is always operated within an enterprise hence **resilience should be conceptualised as an emerging property of the CI enterprise, which includes the CI**. Much more needs to be said about complexity, uncertainty and resilience but this outside the scope of this article.

Security Architecture

An architecture is the "*fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution"* (ISO/IEC/IEEE42010, 2011). The infrastructure ecosystem exists at a national level and therefore has only one architecture instance. The CI enterprise-level security architecture, however, has multiple instances and would benefit from a reference security architecture. A reference security architecture is a generic architecture model intended to be tailored to a specific context and set of security risks. A security reference architecture allows:

- Infrastructure enterprises to manage risk while allowing knowledge management and cost savings for Government;
- Instantiation of a Security Architecture based on the specific CI (or CI complex), the geographical distribution and the nature of risk;
- Designing and managing individual enterprise-level security measures for low, medium, high-risk categories.
- Managing the various risk types through the design of operational concepts, capability elements and any or all their relationships;
- Designing, managing and coordinating across the infrastructure, enterprise and ecosystem levels of security measures; and
- Moving from compliance, which is focused on minimum requirements, to a risk-driven design for individual CI. Quality of the security capability is based the requirement for the CI specific security capability.

[2] The Oxford English Dictionary definition of *any*: "*used to refer to one or some of a thing, no matter how much or how many.*"

A brief overview of the process for developing a CI enterprise-level security architecture is presented in the following subsections. Such a process consists of two main parts, namely understanding the CI security problem and developing the solution. Implementing the architecture is important but is not discussed in this article. Once several representative CI enterprise-level security architectures have been developed and implemented, the reference security architecture can be abstracted from these. There are many issues that must be considered to manage an architecture model that would be required which are also not dealt with in this article.

In developing the enterprise-level security architecture, the appropriate vertical and horizontal integration of the security architecture must be designed. The vertical integration is between the enterprise level and the ecosystem (up) and the elements of the capability (down). The horizontal integration is between the enterprise-level security architecture and other enterprise processes and capabilities.

Understanding the CI security problem

Understanding the CI enterprise security problem requires several important processes:

- Understanding the context of the CI enterprise in the ecosystem;
- Integrated analysis of legal and other constraints;
- Defining measures of CI effectiveness as introduced in the section CI, EI and an infrastructure ecosystem;
- For CIPA risk categorisation, assess the CI output risks;
- Assess CI security risks as described in the section Threat and Security Risk and interpret these risks; and
- Develop scenarios under normal CI operation and for the various risks under different *modus operandi* used for developing and validating the solution.

Developing the security solution and the security architecture

The first and important step in developing the solution is the development of an operational concept (strategic, operational, and tactical). The operational concept describes what the security capability must do (as a whole) to solve the security problems in the context. For threats where there is malicious intent[3], the design of the security operational concept balances risk and cost based on a threat risk appetite arising from the CI Categorisation (Figure 8). For each actor with intent against a resource or asset, with a particular *modus operandi*, an individual security operational concept is developed. The total security operational concept emerges as each of the individual concepts are integrated. For CI categorised as high risk in terms of CIPA, there will be a low threat risk appetite with higher cost implications that for a CI categorised as low risk.

Using the scenarios, various functions are identified and coordinated to address various threats, of which a partial example is presented in Figure 9. This example shows a functional model for a dynamic response to various threats. The first level of securing CI is to demarcate legal and security boundaries, and then deter and delay a potential threat in the form of a physical attack on the infrastructure. Delay must be coordinated with detect to engage a response when an anomaly is detected and classified as a threat or if there is uncertainty. The delay must be matched to the response time.

[3] It is possible to extend this to hazards, all though this is not shown here due to space constraints.

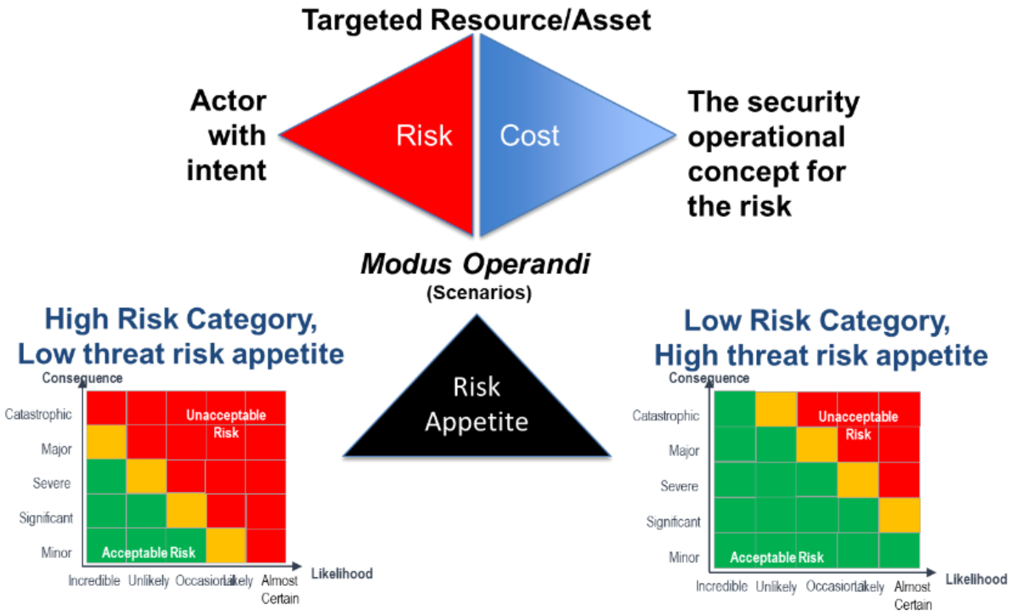


Figure 8. Balancing threat risk and cost in the context of CI Risk Categorisation

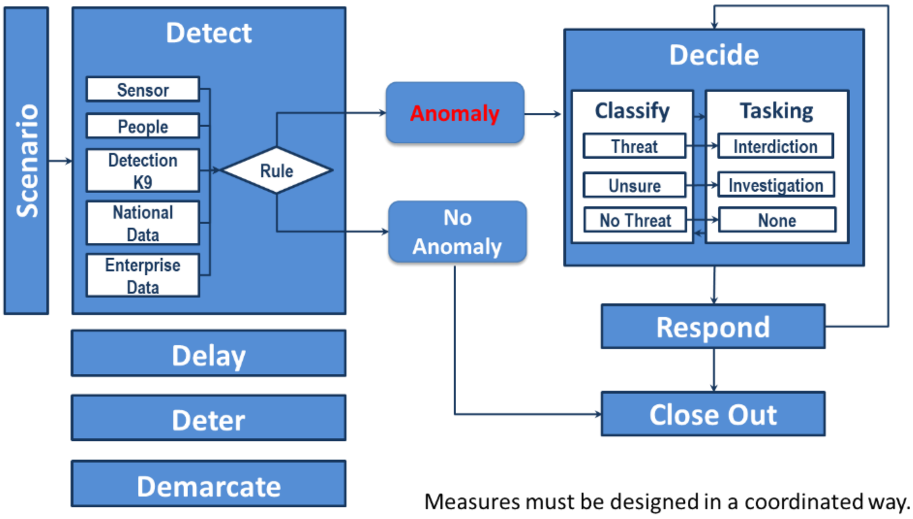


Figure 9. Example of an incident response security operational concept

A key concept in this operational concept is that any detection results in either an anomaly or no anomaly. Firstly, as the fire at Parliament illustrates (News24, 2022), based on available information, the perpetrator was recorded on camera but was not detected. Thus, having a camera or any means of detection is not useful unless it constantly being monitored. But with the number of sensors and other information it is not possible for security personnel to be monitoring all information all the time. Secondly, a detection results in an anomaly and not the declaration of threat because it is not certain that the detection is a threat. Given this situation, and based on the information, a decision could be made that there is a threat. However, additional information may be required, and for which additional sensors are required.

The operational concept is the first level of the enterprise security architecture. As the design proceeds, the elements of a security capability are chosen in a balanced way:

a) **Principles** used in the design of the security capability.
   - Layered defence, zoning.
   - Principles of resilience

b) **Governance**
   - Legislation and regulations;
   - Security Policy and Plans and
   - Governing committees.

c) **Organisation, structure and personnel** relating to security
   - Number of people and how they are organised;
   - Roles and responsibilities;
   - Static and dynamic re-organisation, especially for resilience;
   - Job descriptions and selection;
   - Integrity management; and
   - Wellness.

d) **Processes and procedures** (including information and performance)
   - Visitor entry and exit;
   - Lockdown and evacuation;
   - Intelligence chain;
   - Command and control processes; and
   - Investigation and internal investigation.

e) **Technologies** - Options and designs for sensors, and other tools and infrastructure that once selected for a particular purpose become the CI enterprise technical systems:
   - Sensors: Cameras, etc.;
   - Data processing;
   - Data recording;
   - Communications;
   - (Uninterruptable) Power supplies;
   - Platforms and
   - Response.

f) **Culture** is shaped through organisational narratives, language, symbols and practices that constitute "how things are done". It should, however, be noted that culture is an emerging organisational characteristic and is not designed in a "rational" way.
   - General security related culture;
   - Resilience culture; and
   - Culture of care for infrastructure.

g) **Leadership and management**: Required support or changes to leadership style and change management.

h) **Training and Learning** to be able to implement the process and use the technical systems safely and securely.
   - Regulations;
   - Governance;
   - Processes; and
   - Systems.

i) **Security related facilities**
   - Gates, perimeter fence and patrol roads;
   - Operations centres;
   - Server and radio rooms;
   - Landing strips, helipads and hangers;
   - Accommodation for personnel;
   - Training facilities;
   - Armory;
   - Maintenance facilities;
   - Storage facilities.

Various candidate architectures should be developed. Selecting the bast architecture out of the candidate architectures will require effectiveness analysis, trade-off studies or experiments.

Conclusions and Recommendations

Interconnected threats at increased levels on the CI and infrastructure ecosystem requires adopting a holistic, forward-looking approach to security risk assessment. For CIPA CI risk classification (S. 19 and 20) is based on its national societal consequences in the infrastructure ecosystem and should exclude input risks. The latter risks will vary with time, but these are not the consequences of losing CI availability. The impact of input risks (common global and national, resource, residual risks etc.) and enterprise risks on the output risk are dynamic and require continuous analysis at CI enterprise- and ecosystem levels. The threat risk appetite and the cost of security measures detailed in the security operational concept will be determined by the CI risk categorisation.

The development of enterprise engineering in various forms provides new opportunities for security engineering. The concept of a security architecture must be considered seriously for securing CI and the infrastructure ecosystem. The security architecture is based on the threat risk while accounting for enterprise and input resource risk which are assumed to be part of normal enterprise management.

If CIPA is to achieve the purpose set out in section 2 of CIPA then:

- Since CI maybe or is dependent on EI, this too must be secured;

- Infrastructure, enterprise, ecosystem and context must all be managed risk in support of CIPA;
- Security measures for a CI enterprise and ecosystem must be coordinated in a Security Architecture;
- Infrastructure with the highest number of dependencies, direct or cascading, is at higher risk than those depending on it; and
- From a stakeholder perspective, we need a whole-of society approach to manage CI enterprises and the infrastructure ecosystem in which they reside.

To allow clear identification of various systems levels it is recommended that definitions be provided in the legislation and regulations for infrastructure, infrastructure enterprise, infrastructure ecosystem, and resilience. Because of complexity and for practical reasons, the principle of resilience should be expanded from infrastructure to an enterprise level. Inserting new technologies (innovation) requires enterprise and employee buy-in and may need to be certified for use in a security environment.

The security risks dynamically inform the design of the Security Architecture through scenarios and the development of a security operational concept. A security architecture allows for the design of security elements in a complete and balanced way that allows management of cost and knowledge. The threat risk, operational concept and security architecture approach proposed requires moving away from compliance to assurance.

References

Beck, U. (1992). *Risk society: Towards a new modernity* (Vol. 17). Sage Publications.

Browne, R. (2021, May). Hackers behind Colonial Pipeline attack reportedly received 90 million in bitcoin before shutting down. *CNBC*. Retrieved from (https://www.cnbc.com/2021/05/18/colonial-pipeline-hackers-darkside-received-90-million-in-bitcoin.html)

CISA. (2019, November). A Guide to Critical Infrastructure Security and Resilience. *Cybersecurity and Infrastructure Security Agency*. Retrieved from https://www.cisa.gov/critical-infrastructure-sectors

DefenceWeb. (2021, November). Mabuza warns on Mozambique insurgency spilling over. *DefenceWeb.*

DefenceWeb. (2021, December). SAMIM forces take down ASWJ terrorists. *DefenceWeb.*

Giannopoulos, G., Smith, H., Theocharidou, M., Cullen, P., Juola, C., Karagiannis, G., . . . Schroefl, J. (2021). *The Landscapeof Hybrid Threats:A Conceptual Model.* Publications Office of the European Union. Luxembourg (Luxembourg): Publications Office of the European Union. Retrieved from https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

Gonçalves, D. P. (2018). Understanding actors in complex security problems. *International Journal of Strategic Decision Sciences, 9,* 1-18. doi:10.4018/IJSDS.2018040101

Haimes, Y. Y. (2009). *Risk Modeling, Assessment, and Management.* New York: Wiley.

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts.* Ashgate Publishing, Ltd.

Hunter, Q., Singh, K., & Wicks, J. (2021, October). *Eight Days In July - Inside The Zuma Unrest That Set South Africa Alight.* Tafelberg Publishers Ltd.

ISO/IEC/IEEE15288. (2015). *Systems and software engineering — System life cycle processes.* Tech. rep., ISO/IEC/IEEE. Retrieved from https://www.iso.org/standard/63711.html

ISO/IEC/IEEE42010. (2011). *Systems and software engineering — Architecture description.* Tech. rep., ISO/IEC/IEEE. Retrieved from https://www.iso.org/standard/50508.html

Kessler, D. J., & Cour-Palais, B. G. (1978). Collision frequency of artificial satellites: The creation of a debris belt. *Journal of Geophysical Research: Space Physics, 83*, 2637–2646.

Mujuzi, J. D. (2020). Electricity theft in South Africa: examining the need to clarify the offence and pursue private prosecution? *Obiter, 41,* 78–87.

NATO. (2021). NATO's response to hybrid threats. *NATO*. Retrieved from https://www.nato.int/cps/en/natohq/topics_156338.htm

News24. (2022). Parliament fire brought under control overnight, parts of New Assembly 'completely gutted'. *News24*. Retrieved from https://www.news24.com/news24/southafrica/news/live-fire-breaks-out-in-parliament-firefighters-battling-to-contain-blaze-20220102

Wall, M. (2021). Space collision: Chinese satellite got whacked by hunk of Russian rocket in March. *Space.com*. Retrieved from https://www.space.com/space-junk-collision-chinese-satellite-yunhai-1-02

Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy policy, 39*, 6100–6119.

Zandee, D., van der Meer, S., & Stoetman, A. (2021). Countering hybrid threats: Steps for improving EU-NATO cooperation. *Clingendael Report*. Retrieved from https://www.clingendael.org/pub/2021/countering-hybrid-threats/2-hybrid-threats-searching-for-a-definition/

Zondo, J. R. (2022). Judicial Commission of Inquiry into State Capture Report.

Biography

Duarte Gonçalves is currently employed by the CSIR as a Principal Engineer where he currently leads the on-going development and application of a whole-of-society approach to security in the areas of disaster management, infrastructure security and wildlife crime. He has contributed to national strategies in wildlife crime and the development of whole-of-government and whole-of-society approaches nationally. In this capacity, he works with a variety of government departments, social scientists, engineers and other experts and has developed experience using transdisciplinary research methods in security for "dealing" with complexity. He has facilitated stakeholder workshops for developing futures and various interventions.

Duarte Gonçalves is a registered professional engineer with a PhD in Engineering Development and Management.

Chris Serfontein is currently employed by the CSIR as the Integrated Defence and Security Manager where he leads collaborative initiatives between public and private security stakeholders in the national security environment. He served in the Department of Defence and commanded and managed specialised operational and technology security programs for government departments. In his current capacity, he works with government departments, private security industry, civil society, and non-governmental organisations involved in national security initiatives. Recently he contributed to national strategies in the areas of multi-national environmental organised crime, critical infrastructure protection, rural safety and combatting of terrorism. Chris Serfontein is a retired Colonel with an MBA.