The Effectiveness of South Africa’s legislative Framework Governing Cybersecurity in Nuclear Facilities

Khaled Ahmad Qasaymeh *

ABSTRACT

Conventional legal framework intended to protect nuclear related-activities focused on the physical protection of nuclear materials. The definition of nuclear materials as contained in the Convention on the Physical Protection of Nuclear Material became inadequate because it covered only plutonium, enriched uranium, and international nuclear transportation. The multidimensional threats to nuclear facilities have become sophisticated and now include non-state actors. The potential exploitation of nuclear vulnerabilities has necessitated the development of a nuclear security regime which is able to prevent, detect and respond to theft, sabotage, unauthorised access and illegal transfer, or other malicious acts involving nuclear material as well as radioactive substances and their associated facilities. The adoption of International Convention for the Suppression of Acts of Nuclear Terrorism in 2005 has globally strengthened the legal regime governing nuclear security. However, the legal framework governing the protection of the extensive implementation of digital systems, for example instrumentation and control (I&C) systems for the monitoring, control and protection of nuclear power plants is still in its infancy, but is evolving. This paper seeks to examine the effectiveness of the existing legal framework governing cybersecurity in nuclear facilities in South Africa.

Keywords: Nuclear, cybersecurity, information, protection, law, admissibility, convention, legality, legislation, evidence.

Introduction

The legal framework governing nuclear security is principally based on the Convention of the Physical Protection on Nuclear Material (CPPNM),1 the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT),2 and the United Nations (UN) Security Council Resolutions 1373 and 1450 adopted in 2001 and 2005 respectively. Initially, the CPPNM focused on the physical protection of nuclear materials and the criminalisation of specific aspects relating to such protection. The legal lacunae left by the CPPNM revolve round two issues:

- The first issue pertains to the definition of nuclear materials as contained in the CPPNM which, definition covers only “plutonium, enriched uranium and international nuclear transport”.3 Consequently, the need to review the effectiveness of the CPPNM in combating illicit trafficking of nuclear materials became an international topic of debate in the 1990s.4 The States Parties to the CPPNM deliberated whether the physical protection during international transportation as provided for in the Convention, required amendment in order to broaden its scope. In 2005, the CPPNM Review Conference adopted an amendment by consensus. The “amendment extends the scope of the CPPNM to also cover nuclear facilities and nuclear material in domestic use, storage and transport used for peaceful purposes, as well as sabotage”5. The International Atomic Energy Agency (IAEA)6 General Conference adopted a resolution entitled “Nuclear Security,”7 in order to encourage the swift implementation of the 2005 Amendment.8 However, the Amendment to the Convention has not entered into force as yet.
- The second issue relates to the failure of the
CPPNM “to differentiate nuclear terrorism from other criminal acts involving nuclear materials”. The CPPNM does not provide for the prosecution of nuclear terrorism, for example for the safety of nuclear reactors, or the possibility “that terror agents can construct or acquire nuclear weapons” or “might build ‘dirty bombs’”. The United Nations General Assembly (UNGA) adopted Resolution 51/210 of 1996 establishing an ad hoc committee as part of the UNGA’s efforts to introduce an International convention for the suppression of acts of nuclear terrorism, an aim that was realised in 2005. The ICSANT extends the definition of nuclear materials to include nuclear facilities and devices, establishes the legal foundation for international cooperation in combating nuclear terrorism, criminalises the possession, use, or threat by any person of radioactive devices to cause death, serious bodily injury, or environmental or property damage, and requires each State Party to take legal measures intended to prohibit and punish crimes that fall within the scope of the ICSANT by imposing “penalties consistent with their grave nature”.

Nonetheless, both the CPPNM and the ICSANT do not cover any aspect relating to the implementation of information and communications and technology (ICT) systems in nuclear facilities. Cyberattacks on nuclear facilities which mainly target computer systems for various purposes seek to expose vulnerabilities within these systems. These attacks, which are aimed at nuclear power plants in particular, may cause the release of radiological materials, thereby having serious and adverse impacts on human life, property, the environment and the economy.

Statement of problem
The legal regime governing the nuclear industry in South Africa is composed principally of the Nuclear Energy Act (NEA) 46 of 1999, the National Nuclear Regulator Act (NNRA) 47 of 1999, and the National Radioactive Waste Disposal Institute Act (NRAWDIA) 53 of 2008. However, these Acts contain provisions of limited scope when it comes to dealing with the security aspects of nuclear facilities as is apparent from the following:

- Section 29 of the NEA deals with the protection of “the installations, sites, premises and land belonging to or under the control” of the Nuclear Energy Corporation of South Africa (NECSA). It further establishes the authority of NECSA to “make any arrangements it considers reasonably necessary for the proper protection” of its installations, sites, premises, land, persons, properties, records and information.
- Section 42 of the NNRA defines the powers of the Regulator relating to the arrangements which are deemed “necessary for the proper protection or security of property which belongs to, or is under the control of the Regulator or is on any premises on which activities of the Regulator are performed”.
- Section 26 of the NRAWDIA duplicates section 42 of the NNRA. The only difference is that section 26 of the NRAWDIA establishes the authority of the Institute to deal with the provisions relating to the security of the Corporation’s installations, sites, premises, etc.

South Africa signed the CPPNM on 18 May 1981 and ratified it on 9 July 2007. In addition, South Africa deposited instruments for ratification of the ICSANT on 9 May 2007. Presumably, the legal measures required by these two conventions have been implemented by the NEA, NNRA and NRAWDIA. Nevertheless, the obligations entrenched in the ICSANT have been enforced by the Protection of Constitutional Democracy against Terrorist and Related Activities Act (PCDTRA) 33 of 2004, which came into operation in 2005. Section 1 of the PCDTRA defines terrorist activity as including “the systematic, repeated or arbitrary release into the environment or any part of it or distributing or exposing the public or any part of it to”, radiation or radioactive materials. However, the criminalisation of nuclear-related offences amounts merely to an exact duplication of the offences as set out in article 7 of the CPPNM and in article 2 of the ICSANT, which offences are incorporated in section 27 of the PCDTRA through the insertion, in the NEA, of section 34A.

Although the PCDTRA incorporates several international instruments which provide for the protection of nuclear materials, section 34A blurs the distinction between terrorist activities and criminal activities. Moreover, although section 1 of the PCDTRA, under the
definition of “terrorist activity” in (a)(vi), covers harm to an electronic system, including an information system, it does not provide for specific governance of cybersecurity in respect of nuclear facilities. In view of the recognition by the Hague Nuclear Security Summit in March 2014 of “the fundamental need to protect the sensitive nuclear information, technology and expertise necessary to acquire or use nuclear materials for malicious purposes, or to disrupt information technology based control systems at nuclear facilities”, this paper examines the effectiveness of the existing legal framework governing the cybersecurity of nuclear facilities in South Africa.

Structure

The notion of cybersecurity at nuclear facilities involves many technical themes, including “the prevention of, detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities”, Nonetheless, a legal framework governing cybersecurity at nuclear facilities is required in order to establish measures for the protection of computer systems, networks and digital systems which are critical to the safe and secure operation of nuclear facilities at various levels. These security measures are also important for the physical protection of nuclear facilities by preventing theft, sabotage and other malicious acts. This paper deals with two focal points, namely the protective measures in respect of nuclear facilities taken during the design stage and intended to combat crimes and terrorism, and the cybersecurity measures intended to deal with cybercrimes and cyberterrorism.

The protective measures in respect of nuclear facilities

The CPPNM and the ICSANT do not provide for measures for the physical protection of nuclear facilities. The exception is article 8 of the ICSANT, which requires states to “make every effort to adopt appropriate measures to ensure the protection of radioactive material, taking into account relevant recommendations and functions of the International Atomic Energy Agency”. The IAEA recommends the development of a design basis threat (DBT) that takes into consideration the attributes and characteristics of the insider and/or external adversaries that have the potential capability to perform malicious acts which may lead to unacceptable consequences. Thus what is necessary is the development of the methods for the design and evaluation of physical-protection systems intended to counter adversaries. This is the responsibility of the state, and the state is therefore required to develop and maintain an adequate nuclear-security regime.

Predesigned physical-protection measures (security by design)

The protective measures taken at the initial stage of building a nuclear facility are dependent on the licensing procedures. South Africa’s nuclear-licensing regime, which empowers the National Nuclear Regulator (NNR) to exercise oversight of safety and security standards, statutorily restricts nuclear-related activities as follows:

- Siting, constructing, operating, decontaminating, or decommissioning a nuclear facility is not allowed by any person, except with a licence.
- All acts which are capable of causing nuclear damage are prohibited, except those nuclear activities which can be licensed.
- The chief executive officer of the NNR who issues the licence may “establish standard conditions applicable to one or more categories of certificates of registration”.
- Any person who fails to comply with the above-mentioned restrictions commits an offence which is punishable by a fine or imprisonment.

These conditions thus place the nuclear industry in the hands of the licence holder. However, such conditions do not provide for specific preventive measures to be incorporated in the design and so guarantee the physical protection of the nuclear installation. Although section 42 of the NNRA covers the NNR’s powers regarding the security of property and premises, the provision is limited to the “security of property which belongs to, or is under the control of the Regulator or is on any premises on which activities of the Regulator are performed”. It is clear that section 42 of the NNRA falls short of the objectives of security by design as most nuclear activities take place within the property of the licence holder.

Combating nuclear-related criminal offences

Combating nuclear-related criminal offences should be differentiated from combating nuclear terrorism. Although nuclear-related offences and nuclear terrorism may appear similar, the motive for committing a nuclear-
related offence is totally different. Nevertheless, the legality of the intervention of the criminal-justice system is a prerequisite for maintaining the effective criminalisation of various nuclear-related offences. “A proactive approach requires the definition of appropriate offences in compliance with the rule of law principle of no crime and no punishment without a law”. That is to say, effective prosecution is fundamentally dependent on the definition of the intentional commission of unlawful nuclear-related acts. Hypothetically speaking, if a person had stolen highly radioactive material and had stored it, thereby causing the death of people living close by who had been exposed to radiation, it would have been impossible to criminalise such conduct or to talk about the grave nature of the act that the person had committed without a fixed and predetermined law decreeing such commission a punishable crime. This situation has now been resolved by article 7 of the CPPNM, which criminalises the following actions:

“1. The intentional commission of:
   a. an act without lawful authority which constitutes the receipt, possession, use, transfer, alteration, disposal or dispersal of nuclear material and which causes or is likely to cause death or serious injury to any person or substantial damage to property;
   b. a theft or robbery of nuclear material;
   c. an embezzlement or fraudulent obtaining of nuclear material;
   d. an act constituting a demand for nuclear material by threat or use of force or by any other form of intimidation;
   e. a threat:
      i. to use nuclear material to cause death or serious injury to any person or substantial property damage, or
      ii. to commit an offence described in sub-paragraph (b) in order to compel a natural or legal person, international organization or State to do or to refrain from doing any act;
   f. an attempt to commit any offence described in paragraphs (a), (b) or (c); and
   g. an act which constitutes participation in any offence described in paragraphs (a) to (f) shall be made a punishable offence by each State Party under its national law”.

The CPPNM obligates South Africa to proscribe the offences set out in article 7 of the CPPNM as punishable by “appropriate penalties which take into account their grave nature”. This has been effected by section 27 of the PCDTRA, which deals with laws amended or repealed. Consequently, the Criminal Procedure Act 51 of 1977 and the NEA have been amended by inserting section 26(1)(j) of the Non-Proliferation of Weapons of Mass Destruction Act 87 of 1993, section 56(1)(h) of the NEA, and section 34A of the NEA. The latter has been drafted as a result of the revision of article 7 of the CPPNM.

The legal problem which emanates from the CPPNM and its implementation is limited to the narrow definition of nuclear materials. Thus, the criminalisation of nuclear-related acts embodied in article 7 of the CPPNM, and, consequently, in section 34A of the NEA, is confined to plutonium, enriched uranium, and international transportation of nuclear materials. This has been supplemented by the Amendment to the CPPNM based on its entry into force.

Combating nuclear terrorism

Combating nuclear terrorism has become a very pressing issue. The ICSANT establishes acts of terrorism as criminal and unjustifiable “by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature” and seeks to ensure that such acts “are punished by penalties consistent with their grave nature”. The ICSANT further states that “acts of nuclear terrorism may result in the gravest consequences and may pose a threat to international peace and security”. Thus, the ICSANT has made significant contributions to the existing legal regime governing nuclear security as follows:

- The expansion of the definition of nuclear materials to include radioactive materials, nuclear facilities, and nuclear and radioactive devices.
- The establishment of appropriate preventive measures to ensure the protection of radioactive materials.
- The establishment of the principle of international cooperation regarding nuclear terrorism.
- The involvement of IAEA beyond its mandate relating to safety.
- The establishment of synergies between non-proliferation and security.

The ICSANT creates legal obligations requiring each
State Party to adopt the following necessary measures:

a. To establish the offences set forth in the ICSANT as criminal offences under its national law.47

b. To take into consideration the grave nature of these offences and accordingly make them punishable by way of appropriate penalties.48

The position regarding the implementation of the ICSANT in South Africa’s legal system is not clear. The PCDTRA takes into consideration several terrorism conventions except the ICSANT. Possibly, this is due to the fact that the PCDTRA was enacted in 2004 whereas the ICSANT was adopted in 2005.

Combating nuclear terrorism is not exclusive to the ICSANT. The United Nations Security Council (UNSC) Resolution 1373 links terrorism with the illegal movement of nuclear materials and establishes mechanisms to implement the Resolution.49 Further, the UNSC Resolution 1540, which was adopted while acting under Chapter VII of the UN Charter, is designed to combat the use of nuclear, chemical or biological weapons and their means of delivery by non-state actors.50 The Resolution establishes the UNSC 1540 Committee to oversee the implementation of the Resolution by all States.51

South Africa reported to the 1540 Committee in 2005, 2006, and 2007. The matrix of national legal frameworks, as approved by the 1540 Committee on 30 December 2010, incorporates those measures relating to biological weapons (BW), chemical weapons (CW), and nuclear weapons (NW) and accounting for/securing/physically protecting such weapons, including related materials. As regards the physical protection of nuclear materials, South Africa reported as indicated in Table 1:

<table>
<thead>
<tr>
<th>Table 1: Report to the 1540 Committee by South Africa on the physical protection of nuclear materials</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OP 3 (a) and (b) – Account for/Secure/ Physically protect NW including Related Materials</strong></td>
</tr>
<tr>
<td><strong>Can violators be penalized?</strong></td>
</tr>
<tr>
<td><strong>National legal framework</strong></td>
</tr>
<tr>
<td><strong>Enforcement: civil/criminal penalties, and others</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Are any of the following measures, procedures or legislation in place to account for, secure or otherwise protect NW and Related Materials?</th>
<th><strong>YES</strong></th>
<th><strong>National legal framework</strong></th>
<th><strong>YES</strong></th>
<th><strong>Enforcement: civil/criminal penalties, and others</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Measures to account for production</td>
<td>X</td>
<td>1. NEA, Chapter III</td>
<td>X</td>
<td>1. NEA, sec 56</td>
</tr>
<tr>
<td>2 Measures to account for use</td>
<td>X</td>
<td>2. Non-Proliferation Act no. 87/1993 (dual-use)</td>
<td>X</td>
<td>2. Non-Proliferation Act no. 87/1993 (dual-use)</td>
</tr>
<tr>
<td>3 Measures to account for storage</td>
<td>X</td>
<td>3. NNRA</td>
<td>X</td>
<td>3. NNRA</td>
</tr>
<tr>
<td>4 Measures to account for transport</td>
<td>X</td>
<td>4. Notice No. 21 of 3 February 2010</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Other measures for accounting</td>
<td>X</td>
<td>IAEA Additional Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 Measures to secure production</td>
<td>X</td>
<td>1. NEA, Chapter III</td>
<td>X</td>
<td>1. NEA, sec 56</td>
</tr>
<tr>
<td>7 Measures to secure use</td>
<td>X</td>
<td>2. Non-Proliferation Act no. 87/1993 (dual-use)</td>
<td>X</td>
<td>2. Non-Proliferation Act no. 87/1993 (dual-use)</td>
</tr>
<tr>
<td>8 Measures to secure storage</td>
<td>X</td>
<td>3. NNRA</td>
<td>X</td>
<td>3. NNRA</td>
</tr>
<tr>
<td>9 Measures to secure transport</td>
<td>X</td>
<td>Monitoring systems to secure facilities in the event of fire or against theft; security personnel in motor vehicles</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>10 Other measures for securing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 Regulations for physical protection of facilities/materials/ transports</td>
<td>X</td>
<td>National Key Points Act no. 102/1980 (NKPA)</td>
<td>X</td>
<td>NKPA</td>
</tr>
<tr>
<td>12 Licensing of nuclear installations/entities/use of materials</td>
<td>X</td>
<td>NNRA, Chapter III</td>
<td>X</td>
<td>NNRA, Chapter III</td>
</tr>
</tbody>
</table>
Table 1 which is based on the Report of South Africa to the 1540 Committee, shows, among other things the legal framework governing the physical protection of nuclear materials. However, the PCDTRA does not feature in this cluster of laws. Yet, the amendment of the NEA by the insertion of section 34A embodied in the schedule to the PCDTRA is intended to protect nuclear facilities and materials according to the precepts relating to criminal acts and acts of terrorism.

In view of the fact that the approval of the 1540 Committee of the matrix of laws focused on the non-proliferation of BWs, CWs, and NWs, it is clear that governance of nuclear security is still unconsolidated. The best way to identify the mushrooming nature of South Africa’s regulatory frameworks governing nuclear security relating to the preventive measures accompanying the design of a nuclear facility, is to examine the aspirations of the NNR as contemplated in its strategic plans. The NNR Strategic Plan 2006-2009 recognised the “increased security concerns after the events of 11 September 2001 in the USA, specifically, security of nuclear power plants and radioactive sources”. One of the deliverables identified was achieving a strategy “for regulatory control (standard, assessment, compliance and inspection) over physical security measures developed and implemented”. The NNR Strategic Plan and Budget for 2008-2011 shifted the NNR’s concerns to the “security of nuclear installations, radioactive sources, illicit trafficking of radioactive material...”. The NNR Strategic Plan and Budget for 2009 -2012 focused on, among other things, the “[strengthening] of the regulatory oversight of nuclear security by developing a regulatory framework and implementation plan for nuclear security”.

<table>
<thead>
<tr>
<th>Are any of the following measures, procedures or legislation in place to account for, secure or otherwise protect NW and Related Materials? Can violators be penalized?</th>
<th>National legal framework</th>
<th>Enforcement: civil/criminal penalties, and others</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>if YES, indicate source document</td>
<td>YES</td>
</tr>
<tr>
<td>15</td>
<td>National regulatory authority</td>
<td>X</td>
</tr>
<tr>
<td>17</td>
<td>IAEA Code of Conduct on Safety and Security of Radioactive Sources</td>
<td>X</td>
</tr>
<tr>
<td>18</td>
<td>IAEA Database on Illicit Trafficking of Nuclear Materials and other Radioactive Sources</td>
<td>X</td>
</tr>
<tr>
<td>19</td>
<td>Other Agreements related to IAEA</td>
<td>X</td>
</tr>
<tr>
<td>20</td>
<td>Additional national legislation/regulations related to nuclear materials including CPPNM</td>
<td>X</td>
</tr>
</tbody>
</table>
Strategic Plan 2012-2017 identifies the regulatory-framework predicament as follows:

“The NNR regulatory framework may not be adequate. This results from insufficient regulatory standards and practices (policies, regulations, requirements, guidance and position papers); insufficient framework standards and expertise; lack of standardised manuals and procedures for authorisation; uncertainties in the overall planning of the nuclear expansion programmes; lack of appropriate provisions in the NNR Act covering nuclear security. The NNR Act is being amended to factor [in] consideration of these issues”.56

Cybersecurity at nuclear facilities
The physical integrity of nuclear facilities is fundamentally dependent on the safe operation of these facilities. “Computer systems, networks and other digital systems”57 are heavily involved in the operation of such facilities. However, these digital systems are susceptible to attack for several reasons including:

- building up a later coordinated attack intended to sabotage the plant and/or to remove nuclear material;
- endangering human or environmental safety;
- launching an attack towards another site;
- creating confusion and fear;
- gaining monetary profit for a criminal group of people;
- creating major market instabilities and gains for selected market players.
- depending on the objectives or aims of the attack, the attacker will try to exploit different system vulnerabilities”.58

Although ICT is critical for the physical protection and the “safe and secure operation of the facility and for preventing theft, sabotage and other malicious acts”,59 the complex structure of legal frameworks governing nuclear facilities focuses primarily on the physical protection of these facilities.

The NNR Strategic Plan 2012-2017 contemplates the legal factors to be submitted by the NNR to the Minister of Energy in order to amend the NNRA. These amendments include among other things, the development and maintenance of a sound organisational infrastructure, which are “motivated by a general inadequacy in our ICT governance”.60 The NNR Strategic Plan 2012-2017 states the following:

“…Some of the risks posed included failure to maintain ICT infrastructure and [overreliance] on third parties. Other risk factors identified included the failure to keep abreast with developments; inadequate understanding of the role of ICT in the organization; inadequate understanding of the legal requirements; inadequate resources; poor maintenance of infrastructure; limited skills to maintain the infrastructure; change in technology; lack of financial resources and planning and lack of integrated change management processes”.61

The IAEA guidance document on security, namely Computer Security at Nuclear Facilities62 suggests that legal framework providing protection for the ICT infrastructure of nuclear facilities should cover: computer-related offences, terrorism, the protection of critical national infrastructure, mandating disclosure of information, privacy, and the handling of personal information.63 In the South African context, the question arises as to whether the available legal framework makes provision for adequate cybersecurity measures to combat both cybercrimes and cyberterrorism attacks directed at nuclear facilities.64

Combating cybercrimes at nuclear facilities
Combating cybercrimes directed at nuclear facilities starts by criminalising all malicious activities which have the potential to cause adverse effects in respect of the safe operation of these facilities. Cyberattackers who exploit vulnerabilities at nuclear facilities are motivated by various reasons.65 The important issue is to differentiate between cyberterrorism, which is an offence committed within the meaning of the ICSANT, and cyberattacks which are offences committed within the meaning of the CPPNM. This differentiation is essential in order to identify the legal framework which criminalises activities, for example unauthorised access to information which causes loss of confidentiality, and the interception and manipulation of information, software and hardware which causes loss of integrity of a nuclear facility and its malfunctioning.

The available framework which provides for legal measures that criminalise interference with ICT systems is
The effectiveness of South Africa’s…

Khaled Ahmad Qasaymeh

The Electronic Communications and Transactions Act (ECTA)\(^6\) 25 of 2002. Prior to the enactment of the ECTA, South African courts were not able to prosecute criminal activities carried out in the electronic environment. This was due to the virtual nature of the evidence and to the nature of cybercrimes themselves. Courts did not admit electronic evidence because such evidence was not legally recognised. This issue is crucial when prosecuting computer offences that require a computerised document to be tendered as evidence. The narrow definition of a traditional document,\(^6\) which was governed by section 34 of the Civil Proceedings Evidence Act 25 of 1965 and by section 221 of the Criminal Procedure Act 51 of 1977, did not cater for digital evidence.\(^8\)

Nevertheless, prosecuting cybercrimes involving electronic evidence in the form of data messages requires both the legal recognition of data messages and a definition of cybercrime. The legal recognition of data messages determines the admissibility of such data as evidence in a court of law,\(^6\) and the definition of cybercrime is required for successful prosecution so that the charge is not dismissed on the basis of *nullum crimen sine lege* (“without a law no charge is possible”), or *nulla poena sine praevia lege poenali* (“no punishment may be inflicted without a penal enactment preceding the crime”).\(^7\)

The ECTA has now solved the problems pertaining to admissibility of electronic evidence in a court of law and pertaining to cybercrimes. Section 11 of the ECTA defines a data message as “data generated, sent, received or stored by electronic means and includes (a) voice, where the voice is used in an automated transaction; and (b) a stored record”. Section 11 of the ECTA thus gives legal recognition, force and effect to a data message in a manner that allows for its admissibility in a court of law. Further, sections 85 and 86 of the ECTA define a cybercrime as including unauthorised access, interception of or interference with any data. Section 86 of the ECTA criminalises the following acts:

1. Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.

2. A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.

3. A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.

4. A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.

5. A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence”.

**Combating cyberterrorism at nuclear facilities**

Cyberterrorism directed at nuclear facilities is predicated on the intention to use computers, networks and control systems to commit the offences enumerated in article 2 of the ICSANT. The requirement that these offences be criminalised is part of the measures designed to prevent or mitigate the impact of such crimes. The problem in criminalising cyberterrorism directed at nuclear facilities lies in the absence of a standard definition of the terrorist act itself, let alone cyberterrorism at nuclear facilities.

The international legal frameworks governing terrorism incorporate a long list of UN resolutions and conventions such as UNSC Resolutions 1373 and 1540, the International Convention for the Suppression of Terrorist Bombings of 1997, the Convention on the Prevention and Combating of Terrorism, adopted by the Organization of African Unity in 1999, the International Convention on the Suppression of the Financing of Terrorism of 1999, the International Convention against the Taking of Hostages of 1979, the CPPNM, ICSANT, etc. However, the definition of terrorism is still mired in endless controversies.\(^7\) Moreover, the guidelines relating to cybersecurity which are incorporated in instruments such as UNGA Resolution 56/183 and the Draft African
Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa are not binding and do not address nuclear facilities specifically.

Nonetheless, the simplest way of evaluating the effectiveness of South Africa’s legal framework governing cyberterrorism directed at nuclear facilities is to examine the PCDTRA. The PCDTRA gives effect to the international instruments dealing with terrorist and related activities\textsuperscript{72} and incorporates UNSC Resolution 1373 into South African municipal law. In the case of \textit{S v Okah},\textsuperscript{73} the Court stated that, “prior to the date of commencement on 20 May 2005 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act No 33 of 2004, it was not possible to try a foreigner in South Africa for misdeeds committed beyond its borders”.\textsuperscript{74} Section 1 of the PCDTRA defines, among other things, terrorist activity as meaning any act committed in or outside the Republic, which:

\begin{quote}
“(vi) is designed or calculated to cause serious interference with or serious disruption of an essential service, facility or system, or the delivery of any such service, facility or system, whether public or private, including, but not limited to—

(aa) a system used for, or by, an electronic system, including an information system;

(bb) a telecommunication service or system;

(dd) a system used for the delivery of essential government services;

(ee) a system used for, or by, an essential public utility or transport provider;

(ff) an essential infrastructure facility; or

(gg) any essential emergency services, such as police, medical or civil defence services;

(vii) causes any major economic loss or extensive destabilisation of an economic system or substantial devastation of the national economy of a country; or

(viii) creates a serious public emergency situation or a general insurrection in the Republic…”.
\end{quote}

The definition of terrorist activity incorporated in section 1 of the PCDTRA, read together with the amendment of the NEA by way of section 34A, establishes a mechanism to prosecute cyberterrorism directed at nuclear facilities. However, the norms governing the nuclear industry appear in the NNRA, the NEA and the NRWDIA.

\textbf{Conclusions}

This paper concludes that, the existing legal framework governing nuclear security and cybersecurity in particular at nuclear facilities is composed of disjointed pieces of legislations.\textsuperscript{75} For example, the implementation of the requirements of the CPPNM by the PCDTRA confuses the line between the legal measures intended to criminalise criminal conduct and those intended to criminalise terrorism. The CPPNM is intended to deal with nuclear-related crimes, while the PCDTRA is intended “to provide for an offence of terrorism and other offences associated or connected with terrorist activities”.\textsuperscript{76} This contradicts the principle of legality which

“prohibits not only the application of ex post facto laws, but also requires that the criminalized conduct be described in precise and unambiguous language that narrowly defines the punishable offence and distinguishes it from conduct that is either not punishable or is punishable by other penalties”.\textsuperscript{77}

The legal predicaments emanated from the implementation of the CPPNM and the ICSANT are comparable to those resulting from the legal framework governing cybersecurity at nuclear facilities. South Africa’s legal framework dealing with cybercrimes and cyberterrorism includes several instruments such as the Prevention of Organised Crime Act 121 of 1998, the Financial Intelligence Centre Act 38 of 2001, the Regulation of Interception of Communication-related Information Act 70 of 2002 etc. Nevertheless, these pieces of legislation do not deal with cybersecurity at nuclear facilities and suffer inadequacy.

The South African Department of Communications drafted National Cyber Policy Framework (NCPF), which was adopted by the Cabinet in 2012.\textsuperscript{78} This policy is intended to address the potential cyberattacks at critical infrastructures which include nuclear power plants.\textsuperscript{79} It recognises that there are various incoherent pieces of legislation which do not establish adequate cybersecurity measures, stating that:
“Currently there are various pieces of legislation, some with overlapping mandates by different Government Departments and whose implementation is not coordinated. Furthermore, the legislation when viewed collective do not adequately address South Africa’s Cybersecurity challenges”.80

In reality, one may conclude that the combination of section 42 of the NNRA, section 29 NEA, section 26 of the NRAWDIA, section 86 of the ECTA, and section 27 of PCDTRA constitutes a legal framework by means of which offences and cyberattacks against nuclear facilities can be prosecuted. However, this legal framework does not achieve the objectives of the CPPNM relating to the aggravated nature of cybercrimes directed at nuclear facilities, nor does it meet the requirement regarding the prevention of such crimes by the licensee. The NNRA, NEA and NRAWDIA do not contain any provision pertaining to the protection of electronic equipment at nuclear facilities. The fact that the aforementioned Acts were promulgated in 1999, 1999 and 2008, respectively, and the ECTA in 2002, may signal the reasons for the legal lacuna relating to cybersecurity in the nuclear industry.

NOTES

(1) The Convention on the Physical Protection of Nuclear Material (hereafter the “CPPNM”) was adopted on 26 October 1979 in Vienna and entered into force on 8 February 1987.

(2) The International Convention on the Suppression of Acts of Nuclear Terrorism (hereafter the “ICSANT”) was adopted on 13 April 2005.

(3) Article 1 of the CPPNM.


(6) Hereafter referred to as the IAEA.


(8) See, article 7 of Resolution 10 of the IAEA General Conference on 20 September 2013, document GC(57)/RES/10; See also, United Nations Disarmament Yearbook, 2013, Volume 38 (Part II) p 194.


(10) Ibid. p 227.

(11) Hereafter referred to as the UNGA.

(12) Article 1.3 of the ICSANT.

(13) Ibid. Article 1.4.

(14) Ibid.

(15) Ibid. Article 2.

(16) Ibid. Article 6.


(18) Hereafter referred to as the NEA.

(19) Hereafter referred to as the NNRA.

(20) Hereafter referred to as the NRAWDIA.

(21) Section 29(1) of the NEA.

(22) Ibid. Section 29(2).

(23) Hereafter referred to as the PCDTRA.

(24) Section 1(1)(a)(ii) of the PCDTRA.

(25) Ibid. Section 1(b)(b).

(26) Ibid. Section 34A reads as follows:

1. For purposes of this section, 'international organisation', has the meaning ascribed to it in section 1 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004.

2. No person may-

(a) intentionally and without lawful authority, receive, possess, use, transfer, alter, dispose of or disperse, nuclear material which causes or is likely to cause death or serious bodily injury to any person or substantial damage to property;

(b) intentionally obtain nuclear material by means of theft or robbery;

(c) intentionally obtain nuclear material by means of embezzlement or fraud;

(d) intentionally demand nuclear material by threat or use of force, or by any other form of intimidation;

(e) intentionally threaten to-

(f) use nuclear material to cause death or serious injury to any person or substantial damage to
property;

(g) commit an act described in paragraph (b) in order to compel a natural or legal person, international organisation or State to do or to refrain from doing any act;

(h) use any nuclear material or device or use or damage a nuclear installation or nuclear plant in a manner which [releases] or [risks] the release of [radioactive] material, with the intent to-

(i) cause death or serious bodily injury; (ii) cause substantial damage to property or the environment; or

(j) to compel a natural or juristic person, an international organisation or a State to do, to abstain or refrain from doing an act; or

(k) attempt, conspire with any other person, or aid, abet, induce, incite, instigate, instruct, or command, counsel or procure another person, to commit an offence referred to in paragraphs (a) to (f)".


(30) Supra. IAEA, 2013, NSS No. 20, p 6.

(31) Section 21(1) of the NNRA.

(32) Ibid. Section 20(3) read with section 2(1).

(33) Ibid. Section 23(1).

(34) Ibid. Section 52(1)(a) read with section 52(3)(a).


(37) Article 7.2 of the CPPNM.

(38) See section 27 of the PCDTRA, which contains the schedule of laws amended or repealed.

(39) Article 1 of the CPPNM.

(40) Ibid., Article 6.

(41) See, the Preamble to the ICSANT.

(42) Ibid., Article 1.

(43) Ibid., Article 8.

(44) Ibid., Article 7.

(45) Ibid., Articles 8 and 18(1)(c).

(46) Ibid., Article 18(1)(b).

(47) Ibid., Article 5(a).

(48) Ibid., Article 5(b).

(49) Articles 4 and 6 of UNSC Resolution 1373.

(50) Article 1 of UNSC Resolution 1540.

(51) Ibid., Article 4.


(53) Ibid., p 15.


(59) Ibid., p 1-2.

(60) Supra, NNR, Strategic Plan of 2012-2017, para 5.2.6.

(61) Ibid.


(63) Ibid., p 10.

(64) Ibid.

(65) Ibid., p 39.

(66) Hereafter referred to as the ECTA.


(68) Taking note that, section 34 of the Civil Proceedings Evidence Act defines the documentary evidence and prescribes its admissibility, and section 221 of the Criminal Procedure Act deals with the admissibility of certain trade or business records. Both sections require the testimony of a person dealing with the evidence in the same manner as an exception to the hearsay rule is applied.


(70) See, supra para 22 of the case of Director of Public Prosecutions, Western Cape v Prins.

(71) For further information relating to the controversy
The effectiveness of South Africa’s…

regarding the definition of terrorism, refer to chapter 2 in Matthew, 2013, Law, Ethics, and the War on Terror.

(72) Paragraph 5 of the Preamble to the PCDTRA reads as follows:

“and whereas the United Nations Security Council Resolution 1373/2001, which is binding on all Member States of the United Nations, as well as the Convention for the Prevention and Combating of Terrorism, adopted by the [Organization] of African Unity, requires Member States to become Party to instruments, dealing with terrorist and related activities, as soon as possible”.


(74) Ibid., para 19.


(76) See, the title of PCDTRA.


(80) Para 22 of the National Cyber Policy framework for South Africa (May 2011).

REFERENCES

Bibliography

Books

Chapters in books and articles

International instruments and treaties
Resolution 10 of International Atomic Energy Agency General Conference on 20 September 2013, document GC(57)/RES/10.

Legislations and Policies
Criminal Procedure Act 51 of 1977.
Electronic Communications and Transactions Act 25 of 2002
Financial Intelligence Centre Act 38 of 2001.
Nuclear Energy Act 46 of 1999.
Regulation of Interception and Provision of Communications-related Information Act 70 of 2002.
South African Nuclear Regulator Strategic Plan and Budget (2008-2011).
South African Nuclear Regulator Strategic Plan and Budget (2009-2012).

Case law
Director of Public Prosecutions, Western Cape v Prins [2012] 3 All SA 138 (WCC) (11 May 2012).

Electronic resources
http://www.iaea.org/About/Policy/GC/GC57/GC57Resolutions/English/gc57res-10_en.pdf
فعالية الإطار التشريعي الجنوبي أفريقي النازم للأمن السيبراني في المنشأت النووية

خالد أحمد قسامية

ملخص

إن الحاجة للتضوير الإطار القانوني التقليدي لحماية المنشأت النووية والأنشطة المتعلقة بها أصبحت ملمحة. ذلك لأن إتفاقية الحماية المادية للموارد النووية نسند على الحماية المادية للموارد النووية، وأن تعريف المواد النووية يشمل البولتيوم، وبارخترومو المخصب، والنقل النووي الدولي فقط. ويتعدد أنواع التهديدات المترتبة للمشادات النووية، وتخلق الجهات القائمة غير الحكومية، التي تتمى إلى استغلال مواقع الضبط النووي المحتملة، أصبح من الضروري تطوير نظام أمن نووي، قادر على منع، وكشف، والرد على السرقة، والتخريب، والوصول غير المصرح به، والنقل غير القانوني، أو أي أعمال خبيثة أخرى تتعلق على المواد النووية، والمواد المشعة الأخرى، والمشادات المتعلقة بها. هذا وقد عززت الإتفاقية الدولية لقمع أعمال الإرهاب النووي في عام 2005، النظام القانوني الذي يحكم الأمن النووي. فتسعت قائمة المواد النووية لتشمل المواد المشعة والمراقبة النووية، وال vagy العناصر النووية والأجهزة المشعة. وتفرض إتفاقية الحماية المادية للموارد النووية والإتفاقية الدولية لقمع أعمال الإرهاب النووي على الدول الأعضاء بذل الجهود اللازمة لتأسس تدابير مناسبة من أجل ضمان حماية المواد المشعة، مع مراعاة توبيات الوكالة الدولية للطاقة الذرية. وقد وقعت جنوب أفريقيا على اتفاقية الحماية المادية للموارد النووية في 18 آب 1981، ووصفت عليها في 9 يوليوز 2007، وأوّدت الاتفاقية الدولية لقمع أعمال الإرهاب النووي للتصديق في 9 أيلول 2007. وتشير جنوب أفريقيا محطة كوبيرغ (western Cape)، وتتكون من مقاطع بقوة 1800 ميجاوات. وتتكون النظام القانوني الجنوب أفريقي، الذي يعين المواد النووي والمراقبة المشددة منها من ثلاثة ترتيبات رئيسية: قانون الطاقة النووية عام 1999، قانون المنظمة النووية المحلي لعام 1999، وقانون المنظمة النووية المحلي للتشريع من الفئات المشعة لعام 2008. غير أن النظام القانوني الذي يلزم الحماية للموارد النووية والمراقبة المتعلقة بها يتوزع على عدد من التشريعات المختلفة، مما يؤدي إلى تشتيت الجهود الراقية إلى تكوين نظام عالي داعم لكل من تسول له نفسه الإعطاء على المواد النووية والمراقبة المتعلقة بها، أو استخدامها على الإعداد، أو استخدامها على الإعداد، أو استخدامها على الإعداد، أو استخدامها على الإعداد. كذلك الأمر، فإن الإطار القانوني الذي يحكم حماية الأنظمة الإلكترونية، والحساسات، وأنظمة القائمة التي تستخدم على نطاق واسع في التشريع، والتحكم، والرصد، والرقابة والحماية في محطات الطاقة النووية، لا يزال قيد التطور، وعلى إقامة الفرقية في خصوصية تصميم إعادة إتفاقية القانوني القائم الذي يحكم الأمن السيبراني الخاص بالمنشأت النووية في جنوب أفريقيا.

الكلمات الدلالية: النووي، الإطار التشريعي، جنوب أفريقيا.

* كلية الحقوق، جامعة جنوب أفريقيا، جنوب أفريقيا. تاريخ استلام البحث 1/3/2015، وتاريخ قبوله 12/6/2015.