INDUSTRY WORKING GROUP ON MULTIPLE TAXATION

BRIEF ON THE DESIGNATION OF TELECOMMUNICATIONS INFRASTRUCTURE AS CRITICAL NATIONAL INFRASTRUCTURE

Table of Contents

1) Executive Summary

The term "Critical infrastructure" is usually employed to describe assets which are essential for the effective functioning of any society or economy. These assets are identified as the basic facilities, services and installations critical to the social and economic well-being of any State. They represent utility assets or 'public works' which are indivisible from the efficient operational activities of any society. It is universally accepted that any nation's health, wealth and security depend upon the production and distribution of certain goods and services. The array of physical assets, functions and systems across which these goods and services move are considered critical infrastructures. Such infrastructures are identified as the most critical to any society and are prioritized based on the level/impact of risk associated with their loss to attack or disaster.

Examples of critical infrastructure are globally accepted to include the following amongst others:

- **Electricity** generation, transmission and distribution;
- **Gas** production, transport and distribution;
- **Oil** and oil products production, transport and distribution;
- **Communications** systems
- **Water** supply
- **Agriculture**, food production and distribution;
- **Public health** (hospitals, ambulances);
- **Transportation** systems (fuel supply, railway network, airports, harbours, inland shipping);
- **Financial Services**(banking, clearing and exchanges services);
- **Security services** (police, military and civil defence).

The essential role played by these in assuring the operation and survival of any society cannot be overemphasised. Accordingly, the global practice is for governments to put in place aggressive policies or programs to ensure the protection of such Critical National Infrastructure (CNI) by guarantying the continued seamless operation and sustainable operations of CNI. These protection strategies are aimed at according CNI physical and virtual protection from both man-made, physical events and acts of nature that could disrupt their provision.

CNI are by nature complex and often interconnected, which means that a disruption in one may often lead to disruption in others. Such disruptions may be caused by any number of factors e.g. poor design, operator error, physical destruction due to natural occurrences (flood, earthquake, etc.), or physical destruction due to intentional human actions (terrorist attacks, theft, vandalism, untoward interventions etc). Protection strategies are thus measures which are taken to guard against and/or quickly respond to these threats. Such measures are designed primarily to improve reliability and safety of CNI. They are also focused on ensuring the continuity CNI in the face of such threats.

This paper will focus specifically on communications infrastructure as critical national assets which warrant the highest levels of protection in view of their significance to the efficient functioning of any society. The importance attached to communications is appropriate in view of its particular supportive role in relation to other critical infrastructures, social and economic activities. Indeed communications can be described as an adhesive which holds other composite systems in our society together. Communications provides the conduits through which interactions between and within other sub-systems, which enable effective functioning of society at large. Therefore a

breakdown in the communications system can lead to a breakdown in many other societal systems which depend upon communication and exchange of information to function successfully. This paper will also consider the best approaches to deliver the CNI status and protection for the Communications Industry. The strategies that will be considered in this paper are highlighted as follows:

Short to Medium Term - Securing an Executive Policy on Critical Infrastructure protection.

- An executive Policy Statement by the President declaring Telecommunications and other critical sectors of the economy e.g. Oil & Gas, Telecommunications, Postal and Broadcasting services, Banking and Health facilities etc as CNI.
- This Policy Statement would accord the requisite protection to CNI under extant legislation and will direct Law Enforcement Agencies and Security Services (LEAs) to enforce the policy objectives of the President of the Federal Republic of Nigeria.
- Formulation of an executive policy strategy document driven by the Federal Executive Council and endorsed by the National Council of State prescribing measures to ensure sustainable operations of CNI, including defined roles for LEAs, public and private sector participants.

Medium to Long Term - Securing Legislation on Critical Infrastructure which will provide amongst other things

- Clear definition of infrastructure to be accorded protection
- Mode of identifying the threats/risks to critical infrastructure
- Create offences for infractions against critical infrastructure
- Severe criminal sanctions for infractions
- Recognition of the need for National Infrastructure Assurance/Protection Plan

In this regard, we wish to draw attention to similar legislation done to provide protection to the petroleum industry, the Petroleum Production and Distribution (Anti- Sabotage) Act No. 35 of 1975, Volume 13 CAP P12 Laws of the Federation of Nigeria 2004. This Act provides for the offence of sabotage which involves the obstruction, prevention of the distribution or procurement of petroleum products. It also extends protection to vehicles (defined to include anything adapted for the transportation of petroleum products by land, sea or air which by extension includes oil pipelines) involved in the distribution; and extends penalties to parties who aid, incite, counsel or procure other person to commit offences specified in this Act. The Act further proposes a primary penalty of not more than 21 years for sabotage. By extension, the IWG proposals seeks to achieve similar protection for the communications industry through Legislation to secure CNI in the best interest of the country.

2) Multiple Taxation and the Telecommunications Industry Experience

The current successes of mobile telephony have been hinged upon by most stakeholders as an opportunity to exert demand and rent seeking opportunities on the telecommunications industry.

While the telecommunications industry has contributed immensely to the socio–economic development (e.g. in terms of job creation, security, social cohesion), improved quality of life and the contribution to Gross Domestic Product (GDP) etc; the telecommunications industry has not enjoyed the requisite privileges and protection it deserves. Majority of industry stakeholders have failed to recognize the role played by telecoms and have continued to hinge on the successes and seek opportunities to short term and other immediate pecuniary benefits. This skewed perception results in undue interference in the operations of communications networks by various strata of society, and particularly agencies of government. These Ministries, Departments and Agencies (MDAs) of Governments continue exert pressure by deploying the very machinery of the State which should by design protect CNI from let or hindrance to enforce an illegitimate regime of taxes and levies against the communications industry. The IWG hereby attaches as Annexure A a table providing a snapshot of this regime of taxes and levies imposed on the telecommunications industry. The failure of operators to yield to these illegitimate demands often results in disruptive enforcement actions by the MDAs, which go as far as forcibly sealing off telecoms sites or removing components of site installations in their bid to compel compliance. Their continued intervention in telecoms operations results in a disruption of services, commensurate increase in operating expenses and the general cost of carrying on communications business in Nigeria. It is the Industry Working Group's (IWG) view that the institution of a definitive framework assuring that due regard and protection are accorded to the telecommunications industry will go a long way towards guaranteeing the sustainability of the Industry.

3) Critical considerations for Securing CNI in Nigeria

Drawing from international best practice and experience on this subject matter, the consistent element includes the institution of a framework which seeks to assure the protection of CNI. The key factors to be considered in providing for such framework include the following:

I. **Definition and classification of CNI** – This paper suggests the expansion of CNI to include telecommunications and other sectors critical to the social and economic well-being of Nigeria such as Oil & Gas, Telecommunications, Postal and Broadcasting services, Banking and Health facilities etc. Inclusion of these sectors will increase support for the objectives of this assignment.

II. **The role of the Public and Private sectors in guaranteeing the sustainability operations of CNI** – The peculiarity of the Nigerian environment and current realities have seen the private sector leading investments in provision of infrastructure support for the provision of most socio economic services which can be classified as CNI. These private sector players are highly regulated by MDAs in the public sector. Therefore to successfully secure CNI in Nigeria, active support and partnership of the public and private sector will be required through a collaborative method which will secure CNI under the policy guidance of the Federal Government of Nigeria.

III. **The designation of a Lead Agency to drive the CNI strategy of the Federal Government of Nigeria**[1] -The IWG recognises the important role played by the Nigerian Communications Commission (NCC) in urging the National Security Adviser to take steps

[1] An example in this regard is the US Department of Homeland Security which was set up as a cabinet department alongside other executive departments to coordinate amongst other things, critical infrastructure protection

to identify the critical network infrastructure within the telecommunications industry. In view of the varying types of infrastructure involved, their complexities and other operational exigencies, this paper proposes that the executive policy document designate a lead agency that will be charged with the responsibility of implementing strategies aimed at securing CNI. This lead agency should be supported in an advisory capacity by a committee of representatives made up of one or two specialists from the relevant industry or industries designated as CNI.

IV. **The development of a robust strategy for securing CNI in Nigeria**[2] - This strategy must amongst other things provide for:

- A broad outline of policy objectives in securing CNI
- Roles of the Public, Private sectors and the LEAs
- Requisite levels of cooperation from all stakeholders
- Detailed steps to protect CNI
- Disaster recovery plans to assure the continuity of CNI in the event of a disaster or attack on CNI etc.

V. Commitment and support of the Federal Government of Nigeria – Government's commitment and support to achieving policy objectives to secure CNI cannot be overemphasised. Government must demonstrate this beyond a policy statement and must provide the requisite environment to assure the sustainability of CNI. While in many jurisdictions Government support had included funding of the lead agency and other arms of Government charged with the responsibility of securing CNI, this paper advocates for a bespoke approach with meets the realities and need of the local operating environment in Nigeria. Government should consider a hybrid approach which could include subsidies, duty waivers and other fiscal incentives which cover the cost incurred by the private sector in securing CNI. While such costs could be made up of additional expenses incurred in importing tools and technology to secure CNI, such fiscal incentives will not absolve the private sector of its responsibility to the treasury in payment of taxes but will augment and encourage private sector efforts to secure CNI. This paper advocates a participatory role for both Government and the Private sector in securing CNI and recognises that any CNI strategy without the full support and commitment of Government will fail to achieve its objectives.

In fulfilment of its obligation to assure the security of lives and properties of citizenry, this paper encourages the government to consider factors proposed in adopting measures to secure CNI.

4) Strategies for Securing CNI in Nigeria

In this regard, the IWG would like to propose the following Short to Long Term strategies which seek to assure that CNI is secured in Nigeria.

[2] Please see for an example the US President's Executive Order EO 13231 Critical Infrastructure Protection In the Information Age 16 Oct 01 http://www.fas.org/irp/offdocs/eo/index.html

1. **Securing an Executive Policy on Critical Infrastructure protection:** This paper proposes that an Executive Policy on securing CNI in Nigeria should be driven by a policy statement by the President highlighting the need to protect identified sectors/industries as CNI. The policy statement should state the overriding objectives and policy thrust of Government (i.e. ensuring sustainable socio – economic development, national security concerns, assuring the continuity of social cohesion, assuring the integrity of critical infrastructure etc.) to ensure the buy in of all Nigerians particularly relevant stakeholders including MDAs and LEAs. The policy statement should lead to a robust Executive policy which should receive the buy in and or endorsement of the National Council of State (which consists of the Governors of the 36 States and past Heads of State and Presidents) The policy should clearly highlight the rational for the protection of CNI, and it should set a national goal which should include the roles of:

    a. The Federal Government in ensuring support for these sectors in their basic operations through the provision of an enabling environment and one-stop shop for approvals and other administrative process
    b. The Federal Government in ensuring protection of these sectors through the deployment of the National Security apparatus in the event that this is required
    c. MDAs, States and Local Government's alignment to the national goal in maintaining the enabling environment required for the delivery of critical services by these sectors
    d. Private sector in ensuring the orderly function of the economy through the delivery of these critical services. These will include amongst other things the obligation of the private sector to use its best endeavours to protect ~~theseinfrastructures~~these infrastructures, provide training and other support to Law Enforcement etc.
    e. Creation of an office for the coordination of Critical Infrastructure Protection; this should probably sit with the Vice President/Presidency and / or National Security Adviser

    The policy should further create a Public-Private Partnership to Reduce Vulnerability. To ensure success, the policy must encourage partnership that is genuine and based on mutual cooperation to the extent feasible. It must seek to avoid outcomes that increase government regulation or expand unfunded government mandates or interventions to the private sector. This may involve:

    a. For each major sector, appointment from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Agency here would be the government MDA responsible for supervision of that sector e.g. the NCC for communications
    b. Identification of a private sector or counterpart (Sector Coordinator) to represent their sector. For the telecommunications industry this could be an ALTON representative.
    c. Under the auspices of the office for the coordination of Critical Infrastructure Protection, the appointee from the Lead Agency and private sector counterpart and organisation they represent shall contribute to a sectoral National Infrastructure Assurance Plan for each identified sector.
    d. This sectoral National Infrastructure Assurance Plan shall assess the risks and vulnerabilities of the particular sector to untoward interventions such as MTR, cyber and/or physical attacks etc. In doing so, the National Infrastructure Assurance Plan shall amongst other things:

- Recommend plans to eliminate significant vulnerabilities;
- Propose a system for identifying and preventing attacks/interventions;
- Develop a plan for coordinating appropriate response to vulnerabilities in the aftermath of an intervention or attack. The office for the coordination of Critical Infrastructure Protection will coordinate response by appropriate security agency (office of the NSA).

e. Creation of an advisory body made up representatives of identified sectors and the NSA to advise the President and Council of State on the subject matter and further ways of enhancing the partnership of the public and private sectors in protecting CNI
f. Include a plan of action to propose a Critical Infrastructure Protection Bill (with input from the Private sector through the office for the coordination of Critical Infrastructure Protection) to National Assembly for passage.

The IWG encourages the use of experienced consultants to develop a framework to achieve the above highlighted objectives The Executive Policy is proposed as a short to medium goal for securing CNI. In the immediate short term, the policy statement from the President should direct LEAs to enforce protection of CNI under extant laws in force in the Federal Republic of Nigeria. The existing laws which could be considered for this purpose are highlighted in the table below as follows:

Legislation	Provision
Nigeria Security and Civil Defence Corps Act (Amendment) Act 2007	**Section 1** provides that Corps can enter and search premises of a suspected illegal dealer in petroleum products or material used by PHCN, Postal Services, NITEL or for any other public utility or infrastructure. **Section 4** sets out the definition of an "act of terrorism" which falls within the ambit of the Corps. The definition includes, "an act which causes extensive destruction to a government or public facility or infrastructure or private property and likely to endanger human life or result in major economic loss".
Criminal Procedure Act	**Section 53** empowers the Police to take pre-emptive action to prevent injury to public property. **Section 55** empowers the Police to make arrests without a warrant to prevent such an offence
Police Act	**Section 10** provides that the President may give to the Inspector General of Police such directions as he may consider necessary for the maintenance of public order and safety.

Public Order Act	**Section 11** empowers the President, on the advice of the Council of state to make regulations for the purpose of achieving the objects of the Act. The objects include maintaining public order.

Comments

- It can be inferred from the above highlighted provisions of the Nigeria Security and Civil Defence Corps Act (Amendment) Act 2007 that " CNI including telecommunications infrastructure" falls under the umbrella of "other public utility or infrastructure" in Section 1 and "public facility or infrastructure…" in the definition of "an act of terrorism" in Section 4.
- The provisions of Sections 53 and 55 of the Criminal Procedure Act can also be broadly interpreted to cover intrusive actions or acts which damage CNI as damage to public property anticipated in the Criminal Procedure Act.
- It is our position that the damage, destruction to CNI or the inability of the CNI such as telecommunications to provide services could lead to the disruption of socio-economic activities. It could further impair the safety and security of millions of Nigerians, affect the ability of LEAs to discharge their statutory function and ultimately lead to the breakdown of law and order. It can therefore be inferred that the President by virtue of Section 11 of the Public Order Act can make regulations with regard to the protection of telecommunications critical infrastructure in order to prevent the said breakdown.
- The same argument with respect to the provision of the Public Order Act can also be put forward with regard to Section 10 of the Police Act.

2. **Securing the passage of a Critical Infrastructure Protection Legislation:** It is proposed that the concerted lobby to secure passage of the Critical Infrastructure Protection legislation should be pursued on two primary fronts. These would involve a Legislative lobby at the National Assembly and an Executive Lobby which will be a fall-out of the proposals to secure an executive policy in 1 above. The Legislative lobby could involve submitting memoranda and convening focus sessions with select committees in the Senate and House of Representatives. As it proposes to expand the focus of CNI beyond the telecommunications industry, such engagement with the legislature could be driven by the NCC (leading discussion), and identified sector regulators (this could work under the auspices of a CNI protection committee which the NCC can set up in parley with other regulators). The NCC is encouraged to reach out to other sector regulators in the Banking, Oil & Gas sectors etc to set up a CNI Protection committee which can serve as a common front for engagement purposes. CNI Protection committee should consist of 1 or 2 members from identified sector-specific regulators and 1 or 2 members from the indentified industry.

   To compliment efforts of the CNI Protection committee the organised private sector (under the platform of existing industry bodies (such as NECA, MAN, Bankers Committee or the NESG or other relevant body). may use the services of strong advocates to ensure a single consistent front to present a position to the Legislature. Modalities to agree on

funding will have to be determined once the common front has been established. However the thrust of the proposals here is to ensure that lobby efforts are done through concerted channels which are designed to ensure the success of the lobby. Engagements on achieving legislation to protect CNI should be seen as a national assignment rather than an industry-specific agenda in order to gain the support of all stakeholders. It is further proposed that the CNI protection committee and the organised private sector should work together to achieve this overriding objective. To collectively achieve this objective, the CNI protection committee should consider the following as key focus areas or agenda:

- Ensuring an informed consultative process – so requisite discussions can be facilitated and inputs provided to committees responsible for drafting and / or review bills at both chambers of the National Assembly.
- If possible submission of a draft Bill.
- Review of existing Bill on CNI and submission of appropriate redrafts to areas of concern in the Bill
- Securing the interest of the identified industries
- Encouraging speedy consideration and passage of Bill into law through sensitisation campaigns and focused lobby efforts
- Liaison between Executive (Attorney General's office), National Assembly and organized private sector to ensure WIN-WIN harmonized position is reached.

5) Conclusion

The IWG urges the urgent consideration proposed in this paper as it thanks the NCC for constituting the IWG and facilitating the process which led to the consideration of these proposals. The IWG makes this submission in good faith and in the overall interest of the industry and the Federal Republic of Nigeria.