The Role of Public Private Partnership on the Implementation of National Cyber security Policies: A Case of Nigeria

*Anthony Kifordu[1], Wilson Nwankwo[2,a *], Wilfred Isioma Ukpere[3]*
[1]Dept. of Business Administration, Edo University Iyamho, Nigeria.
[2]Centre for Professional Training and Development, Edo University Iyamho, Nigeria.
[3]Faculty of Management, University of Johannesburg, South Africa

Abstract- Compared to other components of the Cyberspace, Cybersecurity is emerging the most prominent domain of concern. The reason may not be unconnected with the geometric growth in in the evolution of new computer-based technologies by the day and the deployment of such technologies for both positive and negative purposes. There are four major areas where Cybersecurity programmes are massively ongoing: Technology Products, Research, Education, and Business enterprises. These four areas are unarguably very vital and affect the socioeconomic development of any society. E-commerce and other sensitive socio-economic ventures are growing but are markedly deterred by security concerns in the Cyberspace. Having regard to the foregoing, this paper examines the ongoing Cybersecurity developments in Nigeria especially as it affects the sectors under review. The argument is that there have not been a significant synergy between the two sectors in promoting Cybersecurity development in Nigeria hence the terrifying spate of cybercrimes amidst the Cybercrime prevention and prohibition laws. We submit that a mutual front propelled by Public Private Partnership (PPP) would go a long way to reducing the spate of these crimes in the cyberspace thus promoting socio-economic development in Nigeria and the sub region. It is also submitted that with the involvement of public and private sectors, the legal frameworks for combating cybercrimes would be enhanced further through the use of joint socio-technical approaches.

Keywords*: Cybersecurity, Public Private Partnership, Policies, Cyberspace, Cybernetics*

INTRODUCTION

Public Private Partnerships (PPP) across the globe assume a stopgap in addressing issues of capacity building and infrastructure decadence in governance. It has opened the frontiers of hope in areas governance has been a challenge in addressing the challenges of the governed in modern times. Appreciable successes of PPP has options in financing, management and maintenance, which most successful government had leveraged on by using these developmental structure to drive her message of good governance home. The collaboration arising from the PPP model brings an equal and balanced relationship for participating entities. Agreeably, it is so because government recognizes the parity and various specialized values, which the public sector can offer and as well as what private sector does in building critical infrastructure. Issues on which of the sectors is better at this point is mundane and obsolete in driving holistic development. This is because, in the practice of governance, Government would want to give the best to the governed by harnessing the benefits of public and private sector participation to achieve this task. The idea is to leverage on where necessary what each sector can bring in driving reasonable development in the society. Fundamentally, government involvement in both sectors is geared towards ensuring the provision of quality infrastructure especially the critical ones such as roads, hospitals, schools, job opportunities and right environment that reflect good governance and promote consistent socioeconomic growth. Furthermore, it ensures that sensitive services or infrastructure are not neglected or left in wrong hands, which may not be committed to good governance, transparency, and accountability stand of the government in dealing with taxpayer’s funds. The domain of Public Private Partnership in Nigeria is not new.

**Corresponding Author: Wilson Nwankwo, Email: nwankwo.wilson@edouniversity.edu.ng*

Article History: Received: April 02, 2019, Accepted: June 30, 2019

The first massive project undertaken through PPP in 1978 was the National Arts Theatre located at the Iganmu area of Lagos. From the late 70s till the return of democracy in 1998 it had appeared that not many projects were embarked by successive military governments through the PPP channel.

As noted by Adekunle [1] Nigerian Government's idea of PPP is two-fold. It is best described as dual convention. On one hand, it is perceived as a well-organized communal service delivery instilled with good administration of peril. On the other hand, though a laudable arrangement, it may exploited to reducing revenue of the government. This may be attributed to uncertainties that may be caused by turbulent global monetary policy crisis in some economies having regard to the fact that most PPP arrangements are long-term partnerships. During the period there is the tendency of having instability in exchange rates, which would affect value of initial investment.

Nigeria also believes that the PPP idea could be applied in the promotion and administration of infrastructure, income generation for non-government sectors wherein some private groups enter into agreement to collect revenue for government. Considering how PPP found relevance as a tool for promoting income, positive administration and upkeep choices during the administration of Olusegun Obasanjo, it may be adduced that the Government engaged dual sectorial participation in driving the dividends of democracy. Its recognition gave birth to the establishment of a regulatory commission for infrastructure concession under President Musa Yardua. The Infrastructure Concession Regulatory Commission (ICRC) as it is called later became a statutory government entity vide the provision of section 14 of the infrastructure Concession Regulatory (Establishment, etc) law [2]. The consistent development in Cyberspace, with its overwhelming applications, has appreciably been touching human lives across all endeavors through various information and communication technologies. However, in the process of creating innovative computing and information technology products that enhance productivity, social wellbeing, and better life, there has been a corresponding rise in the spate of insecurity in the use of these products especially those that are connected with the cyberspace. Dasuki[3] noted that the insecurity associated with the cyberspace poses an equal but superior risk elements capable of collapsing economies and their securities as most classified data can be hacked, accessed and used by cyber criminals who may not be traced or tracked. This nature underscores the faith and justification of PPP in a connected economy.

Without such challenges the cyberspace would be a safe haven as it has shown its potency to drive remarkable growth in the economy, creating a new world order without limitations, free and easy access to communication across the globe, efficient means of processing and synthesizing ideas for human development, growth, and sustenance. In its resolve to fight the growing spate of cybersecurity challenges, the Cybercrimes bill [2] was accented to by President Jonathan and became the principal cybersecurity statute in 2015. The said legislation gave statutory backing to National Cybersecurity Strategy earlier developed in 2014. The legislation had demonstrated the government's determination to making the cybersecurity policy and application, tenable, lively, strong and reliable for the teeming public. The principal legislation provided for proactive protection of national interest, assets, critical infrastructure, critical national information infrastructure, encouragement of peaceful interaction and quick responses to issues relating to cyber infrastructure. The Cybercrime legislation was applauded in many quarters for its flexibility and coverage of notable crimes in the cyberspace. As the acceptance of PPP has continued to gain relevance in economies across the globe particularly in terms of collaboration on vital public infrastructure and services financing, it is submitted that Cybersecurity infrastructure and associated services could tap from the stream of PPP offerings. The disconnect between PPP and Nigeria cybersecurity policies is the thrust of this paper which harps and advocates on the synergy between the two which if effectively harnessed could boost national development through capacity building. The objectives of this paper are:

i. Examine the Cybersecurity policies in Nigeria.
ii. Appraise PPP initiatives' effectiveness as a tool towards National Development in Nigeria's Cybersecurity infrastructure
iii. Relate Cybersecurity in other climes to the development of infrastructure in Nigeria.
iv. Proffer real life answer to any successful impediment of PPP as a vehicle to building cybersecurity infrastructure and capacity

LITERATURE REVIEW

2.1 Public Private Partnership (PPP)

According to Daba[4], PPP contextually, "is a function of an established (Lawful, Asset, Public acquisition, etc) domain you are drawing from". The above is similar to the views expressed by National Council on PPP [5], Nepal National Planning Commission [6], Colversion[7], Nigerian National Cybersecurity Strategy and Procurement[8] and Izuwah[9] on PPP. Ordinarily, a PPP is a binding covenant involving public entity (usually a government agency) and a private entity with obligations on both parties, the collective effort of which is geared towards the delivery or maintenance of public infrastructure. As part of the agreement, perils are also shared to the extent the provisions in the covenant [5]. The idea is to achieve a perfect mix of best capacities to get public satisfaction through a mutually beneficially arrangement. With the aim of closing wide Infrastructure gap, small and depleting government resources there is an urgent need for alternative funding of critical infrastructure.

According to Colverson[7]], PPPs may include:

i. Contract relationships/agreements on long term basis
ii. Components of funding is private
iii. Infrastructural or service provision is private
iv. Private sector gets a defined visible risk elements transferred to them in the form of operations, investments, construction as well as design
v. Composite responsibilities in across the period and life cycle that cannot be determined like from finance to construction
vi. State control returned at the end of the relationship cycle;
vii. The transfer of the power of attorney by state to private sectors to provide some critical services when agreements are struck and trust ensured officially

National Planning Commission, Government of Nepal (2011) clearly stated that PPP is:

> *"A combination of assets and resources between private and public assets aimed solely at providing most efficient and effective cost means to deliver and add value more significantly than the old method to the people."*

Izuwah[9] had identified seven conditions for successful definition of PPP, to include:

i. Prearrangement- Among community & secluded understanding
ii. Service provision through a non-government means for the enjoyment of the governed public.
iii. Private partnership management and investment of public service investment
iv. Sharing risks- Optimality in risk sharing by parties having different but same contractual interest
v. Standards -Focus on quality of service / performance
vi. Receipts of income- tied to activity.

2.2 Legal and Policy Framework for PPP in Nigeria

The following legal frameworks and policies on PPP have been recognized in Nigeria:

i. The ICRC Act (Establishment etc,), 2005.
ii. National Policy on Public Private Partnerships (NPPPP)
iii. Presidential Circular [10]: this circular is to the effect that all Ministries, Departments, and Agencies (MDAs) are mandated to engage with the Federal Ministry of Finance (FMOF) and ICRC prior to commencing PPP projects. MDAs were required to establish PPP units
iv. National Policy on Public Procurement[11]

The adoption of PPP in Nigeria under the administration of President Mohammed Buhari 2015-2019 has witnessed has made some remarkable inroads in the following areas: Airport, rail, roads, ports-conveyance sector; tunnels, bridges, Marine resources – from filtration to treatment; Travel-development of facility, wellbeing-particular or general hospitals. Accommodation for unique services- security and judiciary legislative buildings; Instructive facilities-educational related; reprimand and correctional services- prisons; facilities for recreation, Agreement hubs, Administration office lodging, Communal accommodation etc.

2.3. Cybersecurity in Nigeria

Cybersecurity Strategies and policy framework in Nigeria according to Oluwafemi & Onoja[12] in its entirety can be summarized as "a means of bringing out a working model of various parts with rules and regulations of stated activities to address Cybersecurity issues". The office of the National Security Adviser [13] is in tandem with the position of Nicholas and Godwin [14].They believe that some components are of fundamental challenges in Cybersecurity. They identified the following issues as matters of very importance in Cybersecurity.

1. Cybercrime – "Cybercrime involves various kinds of criminal assisted cyber activity which is directly or indirectly assisted by cyberspace and the fundamentals". Besides, most commonly aided fundamentals of cybercrimes involves, malware, attacks, email, scams, virus dissemination, identity threat, cyber bullying, computer assisted forgery, stalking and cyber bullying.

2. Intelligence in Cyber– This is where artificial intelligence plays the role of surveillance without involving human presence.

3. Terrorism of cyber – This is notable in modern era because with improved technology, dangerous attacks on human beings have been witnessed across the globe and it remains unabated.

4. Online Exploitation of Minors- A situation not far from pedophile. It has been widely condemned by the global community involving taking clear advantage of minor who they find on social media using them as victims on social media.

5. Hacking – This is a sophisticated means of using the social media or internet to cause all forms of civil unrest, disrupting how properly processed data should flow.

ENISA [15] came up with its unique methods of dealing with this menace. They include:

i. Lined method: A methodological cycle that runs from development of initial strategy,
ii. Implementation, assessing and elimination or reproducing similar strategy.
iii. Lifespan method: The difference from lined method is it allows for evaluation before review or termination or adjustment
iv. Mixed method: This is a combination or thorough strengthening of various approaches that drives all forms of strategy by strengthening the parts it can go.

S**trategy Action Plan in Nigeria**

i. National Cybersecurity Governance, Coordination and Assurance Mechanism.
ii. Legal and regulatory framework
iii. National cyber incident management framework;
iv. Critical National Information Infrastructure (CNII) Protection and Resilience;
v. Cybersecurity Awareness Campaign and Child Online Protection;
vi. Cybersecurity Capacity Building and Manpower development;
vii. Public Private Partnership;
viii. Assurance and Monitoring

2.4 Strategies and Policies on Cybersecurity: Experiences from other Countries

2.4.1 Japan

Primarily, the security approach used here was a protective measure against any kind of attack. They applied caution on developing unique plans for the duplication and implementation of cyber information used nationally [16]

2.4.2 France

Adopted a sweeping defensive strategy considering specially her national sovereignty, citizens, with a view to protecting critical national information organization [17]

2.4.3 Kenya

The y understand that Kenya is at a tender or young stage as regards Cybersecurity. But its major focus is on protecting all information of national concerns against unforeseen attacks when must occur as a result of the progressive stages being witnessed [18]

2.4.4 Canada

Canada considers cyberspace security issues from a far point of view along major key architectures of government. This is visible from three perspectives of government protecting their own systems and organization, collaboration to keep safely all major systems used away from central government and assisting citizens of Canada remain safe online. The idea is to check attacks in three folds as well as the activities of security agencies by the system and cyber spying, deployment of internet by gorillas, and cybercrime [19]

2.5. Effectiveness of PPP initiatives as tool towards National Development in Nigeria

The Nigeria PPP initiative has witnessed in continuation successes in the following areas:

Roads [20**]**

- Phase 2 of the bridge(Niger)
- Expressway(Lagos/Ibadan)
- Shagamu-Benin-Asaba Expressway(Upgrade and resurfacing)
- Abuja – Kaduna – Kano Dual Carriage Road (Reconstruction)
- Ibadan – Ilorin - Tegina - Kaduna Highway(Dualization)
- Enugu to Port Harcourt Expressway (Total upgrade)
- East West Road 8. Reconstruction and Upgrade of Aba-Ikot Ekpene– Calabar(upgrade)

Ports

- Lagos(Kirikiri, I and II terminal)
- Water Port(Lekki-Deep Water)

- Bakassi & Ibom (Ports-Deep water)
- Sea Port(Badagary)
- Anambra State(Inland, Onitsha Container Depot)
- Delta State, Asaba(CFS)
- Anambra State (Container Depot, Nnewi Inland)
- Gombe State(CFS, Gombe)
- Osun State (Inland Container Depot, Dagbolu)
- Kebbi State(Inland Container Depot,Lolo)

Rail

- NRC (Narrow Guage)
- New Standard Guage (Standard Lines-New Guage)
- Rail, Lots 3 and 1A(Light Rail, Abuja)
- City Buses(Rapid Transit)
- Airports(Kano, Lagos, PH & Abuja)
- MRO(Aircraft) Facility
- NNPC Pipeline and Depot System

2.6 Issues in Cybersecurity in Nigeria

i. Over dependence in ICT for private, commercial and Administrative activities;
ii. Loopholes around Spying, Security Agents and the nation's security apparatus,
iii. Missing motivation to reform sectors conducting public services
iv. Poor attitude towards private sector reforms in that has turned out to be a norm rather than abnormality.
v. Disjointed regulatory responsibilities not spelt out –poor growth of usable network; no good access; content not regulated; protection of FDI at an abysmal level , etc
vi. International Community unwillingness to be involved creatively – However, worthy of note is the effort of the International Telecommunications Union[21],[22] which should be emulate by other key players in the Cybersecurity drive.
vii. Dishonesty and insecurity

METHODOLOGY

This paper addresses the role of community and secluded partnership on the implementation of national Cybersecurity policies with Nigeria in perspective. The research entails the review of PPP in Nigeria, its implementation successes, the cyber policy and strategy, and what obtains in other countries. The approach adopted is an original appraisal of some efforts and researches along the objectives in the research area. To buttress our analysis, cybersecurity strategies in other countries were reviewed specifically Japan, France, Canada and Kenya. This is followed by a review of the successes, and challenges of PPP in Nigeria. Subsequently, the national (Nigeria) security strategy on cybersecurity was assessed along other countries to reconcile PPP gaps using the Nigerian story.

DISCUSSION AND FINDINGS

4.1. Gaps in PPP and Cybersecurity in Nigeria

Having regard to the Cybersecurity issues and access adumbrated in the Nigeria Strategy Action Plan, we have identified the following gaps:

a. Whereas PPP is viewed as a key instrument to deal with Cybersecurity, it is also regularly been prepared to address other serious national security threats both internally and externally adopting traditional and non-traditional approaches, this procedure is exceptionally tricky and unacceptable .
b. Weak and clumsy political will on the part of the ruling class clearly defining the objectives of the PPP collaborations is a challenge. Thus, their inability to push for stiffer measures on cybercrime using constitutional empowerments and provisions as well as the postures of the private sector operators in taking responsibilities cannot clearly outline the collaboration paths, .
c. As a state, their level of delegating this critical national security issues to private sectors also leaves a lot to be desired in that it exposes their inability to address and provide the right direction for issues of Cybersecurity threat which id beveling the nation's security organization. This arrangement has deep rooted implications for a country Cybersecurity issues and the citizens at large.

d. The advancement witnessed through developments in technology begins to undermine a state that has left her Cybersecurity control in the hands of private sector which have dire consequences for matters of security ; especially with the era of control and increasing private ownership

e. Strategies on National Cybersecurity openly identify views persons who will want to get involved and pose threats such as: offenders, guerillas, antagonistic nation, etc. The trio of hateful performers usually considered as present in an outline of offline violence and hostility where it is likely to classify a culprit and, consequently, their incentive.

f. For online where it can be covered from the beginning , the differences have less meaning because they are part of our legal and political system that has eaten deep into the fabrics of our society which has made it very difficult to view and deal with

4.2. Suggested Solutions

Based on the reviews from Cybersecurity Plan [23], Legislative frameworks, Cybersecurity issues in Nigeria, etc. this paper has made the following suggestions:

a. Unpacking the assumptions on security information restrictions in Nigeria that values that are vital towards understanding policies and goals which are specific and embedded to shape the public private collaboration.

b. It is germane to note that this disconnect between parties concerned (public & private) as it relates to responsibilities, parts and power of control is of essence. Particularly when you consider the unique nature of organizing national security, it is not just a model or design, but a key security issue. Summarily, irrespective of the nature of PPP, collaboration, as documented in the policy of government, it is obvious that the partnership will eventually collapse as it won't be sustainable and strong enough to address security issues of national concern.

c. Relationships between the communities on espionage, defense relations and business sectors to encourage involvement of public private partnership is also a factor that will be positive at the long run if encouraged.

d. Let us be aware again that PPP on national security concerns in cyber technology is multidimensional. The various ISPs are in relationship with Government, providing services (Social media) including NGOs, enforcement agencies etc. Considering the documents guiding Cybersecurity issues, PPP often undermines this intricacy because it views itself as a monopolistic entrant which ultimately affect the entire process of adding value and support to security apparatus of government. Government should unpack such idea and work with these ISPs more closely in addressing security threats.

CONCLUSION

There has been an increasing awareness on cybersecurity in recent times as never before in the history of the country. The Economic and Financial Crimes Commission, an agency of the Federal Government, is now recording some success in trapping and securing convictions against cybercrime offenders, it is interesting to note that such has not reflected the true position of cybercrime cases in Nigeria nor has it really curtailed the spate of such crimes. Threats posed by cybercrime by guerillas sponsored and premeditated keeps evolving and gaining momentum on daily basis. In the minds of stakeholders and decision makers across several sectors, more efforts are needed to properly place the cybersecurity agenda of the nation having regard to the global posture of cybersecurity programmes vis-à-vis the Nigerian economy.

Currently, cybersecurity is a priority nationally, with the understanding of PPP as a means of giving better administration and accountable leadership to the people over persistent threats.

Despite some recorded increase in cybersecurity-related PPPs over the past decade, it appears that PPP has become inevitable for developing and developed economies[24] hence this paper concludes that sincere actions are more likely to end up in a failure due to nebulous agenda that lacks vision and improper strategy often hurriedly implemented without articulating application of intelligence, measurement, and control. In other words, an aim not an instrument is buttressed.

The Office of National Security Adviser (2017) has clearly identified measures to address the cybersecurity concerns in Nigeria to include: enforcement of the Cybercrime Act[25], Critical Infrastructure Protection Plan, Building Resilient Manpower and Protection Plan[26], Cybersecurity Assurance and Unified Measure, Child Online Protection and Exploitation Plan, etc. There is need to integrate all private sector, ISPs, Government and the people in the policy framework.

RECOMMENDATIONS

Nigeria has a fast growing population and there is a growing demand for increased critical infrastructure that would require the continuous intervention of PPPs to actualize in the face of Cybersecurity challenges. In the light of the foregoing, this paper recommends as follows:

1. The adoption of an inclusive security framework that will include the ISPs, Private and Public sector participators. This will unpack all the assumptions about national security and give increased protection to PPP in Nigeria.
2. Nigerian government should promote and increase intelligence sharing with the private sector in the domain of national security to address the disjuncture where information is not at the disposal of the users.
3. The government should encourage a framework for numerical identification development that will continue to evolve and forestall any form of threat that can emanate either through or from any citizen directly or indirectly capable of destabilizing national Cybersecurity system.
4. To ensure effective monitoring, collaborations between government and ISPs should be encouraged as it helps to monitor and control activities in in the cyberspace
5. Involvement of PPP in the Cybersecurity architecture without any ambiguity in Cybersecurity issues even when it is treated as a national security in other countries [27].

REFERENCES

[1] A.M. Adekunle, “Public-Private Partnership as a Policy Strategy of Infrastructure Financing in Nigeria”[online] http://njpg.pactu.edu.np/njpgfiles/4-animashaun-mojeed-adekunle-public-privatepartnership-as-a-policy-strategy-of-infrastructure-financing-in-nigeria.htm.

[2] Infrastructure Concession Regulatory Commission (Establishment, etc.) Act, 2005

[3] M.S. Dasuki, “”National Cybersecurity Strategy, 2014

[4] P.D. Daba, “Public-Private Partnership: The Answer to Nigeria’s Development Challenges”, *Journal of Economics and Sustainable Development,* Vol.5, No.22, 2014

[5] National Council on Public Private Partnerships, United States, 2013

[6] Government of Nepal’s National Planning Commission, “White Paper on Public Private Partnership” (PPP), 2011

[7] S. Colverson, “Sustainable Development: Is there a Role for Public–Private Partnerships? A summary of an IISD Preliminary Investigation”, 2011. http://www.iisd.org/markets/procurement.

[8] Office of the National Security Adviser, National Cybersecurity Policy and Strategy, 2018

[9] K. C. Izuwah, “Public Private Partnership – an imperative for Nigeria’s development”, ICRC, Abuja, Nigeria, 2017

[10] Office of the Presidency, “Presidential Circular on Public Private Partnership Projects”, Abuja, Nigeria, September 2013

[11] Bureau of Public Procurements, “National Policy on Public Procurement”, Abuja Nigeria

[12] O. Osho & D. A. Onoja, “Cybersecurity Strategies and policy framework in Nigeria”, International Journal of Cyber Criminology (IJCC), Vol. 9, No. 1, pp 120–143, 2015. 120–143. DOI: 10.5281/zenodo.22390

[13] Office of the National Security Adviser, “Action plan for implementation of the national cybersecurity strategy”, Abuja, Nigeria, 2017

[14] C. F. Godwin, J.P. Nicholas, "Developing a National Strategy for Cybersecurity: FOUNDATIONS FOR SECURITY, GROWTH, AND INNOVATION”, Microsoft, 2013 http://download.microsoft.com/download/b/f/0/bf05da49-7127-4c05-bfe8-0063dab88f72/developing_a_national_strategy_for_cybersecurity.pdf

[15] European Network and Information Security Agency, “Cyber Europe 2012: Key findings and reports”, 2012

[16] Information Security Policy Council, “Information Security Strategy for Protecting the Nation”, Tokyo, Japan, 2010. www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf

[17] Information Agency on Security and Network, France, 2011

[18] Government of Kenya, “Cybersecurity Strategy”, 2014. http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national cybersecuritystrategy.pdf.

[19] Government of Canada, “Canada’s Cybersecurity Strategy”, 2014. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-sctr-strtgy/index-eng.aspx.

[20] Infrastructure Concession and Regulatory Commission, Abuja, Nigeria

[21] ITU (2009) Cybersecurity Guide for Developing Countries, Geneva, Switzerland

[22] ITU (2013) Electronic Crimes: Knowledge-based Report. Establishment of Harmonized Policies for the ICT Market in the ACP Countries., pp1. Geneva.

[23] Federal Government of Nigeria, “Action Plan for the Implementation of the National Cybersecurity Strategy”, Office of the National Security Adviser, Abuja, 2014

[24] S. Colverson, “Harnessing the Power of Public-Private Partnerships: The Role of Hybrid Financing Strategies in Sustainable Development.” http://www.iisd.org/markets/procurement.

[25] Cybercrime (Prevention, Prohibition, etc.) Act 2015

[26] S. Bae et al, "Evolving US Cybersecurity Policy:A Multi-stakeholder Approach" in Task Force Report Winter[M. Aina & E. Jung eds, Henry M. Jackson School of International Studies, University of Washington, Seattle. https://pdfs.semanticscholar.org/930d/02acc241f72fd625a407ddded45be47488b6.pdf

[27] European Commission, "Cybersecurity Strategy of the European Union:An Open, Safe and Secure Cyberspace", JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL,THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Brussels, 2013