Report from the Cybercrime Prosecution Unit

The Cybercrime Prosecution Unit (CCPU) was established to serve as the cybercrime prosecution and cybersecurity policy arm of the Federal Ministry of Justice. The establishment of the CCPU was in recognition of the fact that cybercrime prosecution is a specialized activity and the need to develop essential technical and human resource capacity for the effective prosecution of those responsible for cybercrimes, as well as advising on cybersecurity policy issues.

Overview of Activities

The CCPU has played a key role in the development and enactment of Nigeria's · cybercrime legislation and national cybersecurity policy. In this regard, the CCPU served the Ministry/nation in several national and international assignments, including:

ECOWAS Technical Committee on Legal and Judicial Affairs/ Experts for Drafting the ECOWAS Directive on Fighting Cybercrime, which finalized the ECOWAS Directive C/DIR.l/08/11 on Fighting Cybercrime for adoption by the Council of Ministers.

Ministerial Committee to Review Bills Impacting on National Security, set up by the HAGF. The review covered the NSA (Amendment) Bill, 2011, Terrorism Prevention ~ Amendment Bill and the harmonized Cyber security Bill, 2011, renamed and eventually enacted on 15th May 2015 as the Cybercrime (Prohibition, Prevention, Etc.) Act, 20

The Unit made inputs and played a key role in the Inter-Agency Committee for Development of the National Cybersecurity Policy and Strategy, 2014-2015, - which finalized Nigeria's first National Cybersecurity Policy and Strategy that was adopted/launched by the President on 5th February 2015. The Head of the Unit, received national commendation for contributions made during the assignment.

Following the enactment of the Cybercrime (Prohibition, Prevention, etc.) Act, 2015, (CPPA) the CCPU re-focused on other key initiatives to enable/drive the full implementation of the Act, such as:

Processed the composition and inauguration of the Cybercrime Advisory Council by the HAGF pursuant to Section 42 of the CPPA. The Cybercrime Advisory Council is a requisite part of the institutional framework for the robust

implementation of the newly enacted Act to operationalize the National Cyber Security Fund established under Section 44 of the CPPA. The HAGF inaugurated the Council on 18th April, 2016 and the undersigned was elected to serve as Secretary of the Council.

Seeking the Federal Executive Council's approval for Nigeria's accession to the ~Budapest) Convention on Cybercrime of the Council of Europe (CETS No.185). This 1s pursuant to Sections 41 (2) and 52 (1) and (2), of the CPPA which vests the HAGF with responsibility for effective international cooperation and the fact that cybercrime and cybersecurity threats can only be checked through effective international law enforcement cooperation. The Federal Executive Council resolved that some infrastructural improvements be put in place before accession.

With the HAGF's approval, the Unit worked with the Executive Secretary of the Cybercrime Convention Committee (T-CY) of the Council of Europe and coordinated a pre-accession assessment visit to Nigeria, which took place from the 24th -26th February 2016. The (T-CY) Delegation led by the Executive Secretary met with the HAGF, Minister of Interior, Ministry of Communications Technology, IGP, Chairman of EFCC, key officials from CBN, NCC, NITDA and private sector stakeholders to gauge institutional preparedness/needs and how to better facilitate the process of Nigeria s accession to the Budapest Convention.

Following CCPU advise on the strategic national benefit, the HAGF submitted Nigeria's request for an invitation to accede to the Convention on Cybercrime on 17tl March 2017, and on 10th July 2017, Nigeria was invited to accede to the Convention on Cybercrime. This gives Nigeria an observer status at the Cybercrime Convention Committee (T-CY) and a priority country under the GLACY + Project of the Council c Europe. The Unit has drafted the instrument of accession for execution and is working on identifying reservations if necessary when Nigeria accedes. Acceding to the Convention now will best serve the nation's strategic interest in fighting cybercrime and improving cybersecurity.

The Unit in collaboration with the International Association of Prosecutors' Glob, Prosecutors e-crime Network (GPEN), the Council of Europe and the ECOWA Commission conducted a Cybercrime Training for Prosecutors and Investigator from

ECOWAS Member States held in Abuja from 24 -26 May, 2016. The training le to the establishment of the ECOWAS Cybercrime Justice Network (ECJN), as an online platform for improving sub-regional cooperation in the fight against cybercrime.

The Unit also facilitated and coordinated the West Africa Cyber Security Initiative B

Lateral Workshop, for investigators and prosecutors from all Nigerian law enforcement agencies held from 25-29 July, 2016 and for judges and legislators held 01-04, August 2016 in Abuja. The workshops were sponsored by the International Narcotics and Law Enforcement Affairs (INL) Section and the Economic Section of the U.S Embassy with resources persons drawn from the US Department of State and Department of Justice, and the Unit.

The Unit, in collaboration with Paradigm Initiative Nigeria (PIN) conducted a one-day cyber capacity training workshop on the provisions of the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015 that touch on digital rights, online crimes and internet freedom on Wednesday, 31st May, 2017, for senior police officers drawn from the 36 States and FCT.

The Unit during the period under review provided training to the judges of the Federal High Court and the Appellate courts under the NCC-NJ I annual workshop on emerging trends in the telecommunications sector.

The Unit coordinated the hosting of the 2nd Annual Conference on Combating Financial Fraud and Cybercrime held 23rd -24th May 2017, in Abuja, organized in collaboration with Digital Forensics Limited. The first edition of the conference held in February 2016.

The Unit has proposed to conduct a bespoke in-house prosecutors' training on the strategic use of electronic evidence in cybercrime and terrorism prosecutions, subject to approval and funding. This is to drive proactive development of new core skills around electronic evidence which now permeates not just cybercrime and terrorism prosecutions, but every sphere of litigation.

The Unit is serving on the National Cybersecurity Taskforce established in 2017 following a directive from the Presidency.

The Unit has also presented papers at various training workshops/symposia enlightening members of the public/stakeholders on the provisions of the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015, and Cybersecurity principles.

International Cooperation and Coordination

Apart from the close collaboration with the Cybercrime Convention Committee (TCY), the Unit collaborates with other stakeholders/partners both at policy development and operational levels in the fight against cybercrime. Some of these include:

The Head of the Unit served on the Commonwealth Expert Working Group on Virtual Currencies, 2015 - that produced the Report on the prevalence and impact of virtual currencies in the Commonwealth, that was presented to the Heads of Governments at the CHOGM, Malta 2015. The Commonwealth Expert Working Group on Virtual Currencies is now working on draft guidelines.

In collaboration with the FBI, Europol and 22 other nations' agencies, the Unit participated in the investigation and takedown of the cybercriminals' black market online forum 'Darkode' on 15th July 2015. No prosecutions resulted in Nigeria though because the two suspects from the forum traced to Lagos had used forged identities in procuring ISP services and could not be identified.

The Unit facilitated/coordinated the establishment of a trusted expedited response 'whitelist' by Facebook for the EFCC, to fast track investigative response in 2016.

The Unit is also in discussing with the European Commission on the development and implementation of a regional cybersecurity project, as well as with the Global Forum on Cyber Expertise (GFCE) following an invitation to join the Forum which is focused on access to cyber capacity building training and best practices amongst its members.

Challenges

Capacity building/training: The Unit's training needs are hampered due to lack of funding. However, in collaboration with partners, the Unit has received some level of cyber capacity training as well as provided training to other stakeholders. Some of these include:

The policy objective of developing a nucleus of specialized cybercrime prosecutors who could be deployed to guide investigations, gathering of relevant digital evidence and prosecutions of cybercrime cases is yet to be realized, due to several constraints.

The CCPU faces the following specific challenges:

- Lack of requisite operational funding and special training for prosecutors in the

THE OFFICE OF THE HAGF PARTICIPATED IN THE 2ND ANNUAL CONFERENCE ON FINANCIAL FRAUD AND CYBER CRIME.

areas of cybercrime offences and procedural law, electronic evidence and digital forensics: Procedures and Court presentation.

- Lack of requisite working equipment such as forensic evidence examination stations and software, basic laptop computers, vehicles and access to journals/on line research resources.
- Lack of trained cybercrime investigators/first responders in the police and on law enforcement agencies results in very poor investigation outcomes a compromised electronic evidence.
- Lack of cooperation and synergy between investigators from various l enforcement agencies and prosecutors invariably results in flawed inconclusive investigations and insufficient or inadmissible evidence worthless for trial.
- Nigeria's non-accession to the (Budapest) Convention on Cybercrime, which the sole international instrument on the subject, is a major hindrance to nu needed international cooperation and technical assistance especially in requests for data/electronic evidence held by international service providers. Access will open the way for improved cooperation in cybercrime investigations.

ANTI-TORTURE ACT 2017