

**A SPEECH PRESENTED BY DCP SAMSON KASSALA  
DEPUTY DIRECTOR OF CRIMINAL INVESTIGATION –  
INVESTIGATION AND CID OPERATIONS DURING THE  
PRESS CONFERENCE HELD AT POLICE BOARD ROOM  
BY CEOs ROUND TABLE ON 25<sup>th</sup> MAY 2009**

The CHAIRMAN OF CEOs ROUND TABLE  
MR. ALI MFURUKI  
MR. GEORGE ALLY from CEOs ROUND TABLE TASK  
FORCE

Reporters - From different Medias.

Ladies and Gentlemen.

It is with great pleasure to have this opportunity and I welcome you all here in this Board room for having a blessing word from our friends CEOs Round Table.

This gathering is for marking the training of three days on Cyber Crime investigation techniques that is now conducted at the Institute of Finance Management (IFM).

Mr. Chairman,

The Tanzania Police Force has received your assistance towards this training at the right time and on behalf of the Inspector General of Police Mr. SAID MWEMA, I thank you very much for

your concern on this new development of crime of which criminals threats to compromise our economy and security as well.

Mr. Chairman,

Rapidly improving telecommunication Industry and multiple use of computers have added to the threat from external sources.

Cyber worriors have gained notoriety in the Media and appear to have gained more acceptability than traditional criminals. The suggestion that the computer criminal is a less harmful individual, however, ignores the obvious.

Historically, economic value has been placed on visible and tangible assets. Tangible assets in the computer environment often have double values. The replacement cost of a piece of computer equipment might represent only a small portion of the economic loss caused by the theft of or damage to that equipment. Of much great significance, are the value and impact of the information lost on the society.

Cyber crime is a very effective and attractive method to disrupt a Government, corporation, Banks and Financial Institutions or any other citizen. Such acts are cheaper than traditional crime methods. A Cyber group might utilize a personal computer,

laptop, and a simple telephone connection or wireless devices to accomplish their criminal acts.

Here, bombs and guns are not needed, but still such activities could have a significant and disruptive impact on society. Further more cyber criminals do not have to undergo physical training on the manufacturing of the explosive. They can study 'on line' manuals to manufacture and develop their ideas from publications on the internet. In the ordinary cause, it is more difficult to trace individuals, because there are no physical barriers such as customs or any jurisdictional boundaries. For law enforcement, it is very difficult to identify someone through a screen name, guest user, or alias. Activities and attacks on information systems can be conducted remotely from anywhere in the world.

As dependence on computer technology grows in Tanzania, Africa and around the Globe, it will be crucial to ensure that the rate of technological dependence does not outstrip the rate at which the corresponding social, legal and political frameworks are developing. It is important to plan security and crime prevention tactics at the same time when the computer technology is being implemented. This means that we should retain one step ahead at all times.

The course is designed such as to provide our investigators effective skills and knowledge that reshape their expertise to identify and utilise evidential intelligence during investigations.

This course with twelve modules marks the milestone in developing cyber crime investigative capacity for the Police. With this initiative, we are guaranteeing you and the public as the whole to provide our professional skills all the time and assure timely and scientific investigation to ensure sustainable security of your properties.

Again, I wish to thank you for your mutual understanding and response to support the Police Force in this initiative and other areas where we may request for assistance.

Thank you for your attention.