Zyber Global

NOVEMBER 2020 | ISSUE 4

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the November (4th) edition of Zyber Global Centre's Monthly Newsletter

Living in the northern hemisphere means that I am now in Autumn experiencing shorter days. It is dark now from just after five in the evening and I am busy consoling myself that at least it's not winter (yet!). Winter is three months of even shorter days and bitterly cold weather. If not for COVID-19 I would have already arranged a number of work trips between now and February to the Southern Hemisphere where it is a lot warmer.

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Spotlight

The interview spotlight this month is on H.E. Dr. Ali bin Fadhel Al-Buainain Attorney General of The Kingdom of Bahrain.

Zyber News

We also have a roundup of the latest international cybercrime news.

Zyber Focus

Feature article on Drugs and Cybercrime (Part 2); by Arsha Gosine, Head of Research.

Zyber Global Events

The next Stay Safe Online Webinar by Zyber Global is on the 30th of November, 2020. Register now to attend.

" I believe the focus should be on the development of legal procedures to tackle crimes and its perpetrators,. ...."

H.E. Dr. Ali bin Fadhel Al-Buainain
Attorney General of The Kingdom of Bahrain.

Continued from page 1.....,,,

Now that we are all working online, I want to invite you to a free webinar at which I shall be speaking, "Effective Access to Electronic Evidence: towards a new Protocol to the Budapest Convention."

This webinar will be held on Monday 9 November 2020 at 15:00 CET. It is jointly organized by the Council of Europe and the International Association of Prosecutors and is open for participation for members of the judiciary and prosecutors from countries of Europe, Africa, the Americas and Asia Pacific.
For further information and to register see: https://www.coe.int/en/web/cybercrime/effective-access-to-electronic-evidence-towards-a-new-protocol-to-the-budapest-convention.

I am also excited to introduce H.E Dr Ali from the Kingdom of Bahrain. whom I have known for a number of years.
Dr Ali was one of the first Board Members of the Global Prosecutors E-Crime Network (GPEN) which is part of the International Association of Prosecutors (IAP). His Excellency has worked tirelessly to promote GPEN throughout the Gulf Cooperation Countries by translating policies and best practice into Arabic. He continues to raise awareness of cybercrime in the region through a joined up approach.

Finally, remember to stay safe on-line by ensuring that you:

- *change passwords regularly;*
- *click smart; and*
- *be a selective sharer especially with your personal information.*

ESTHER GEORGE
Editor and CEO Zyber Global Centre

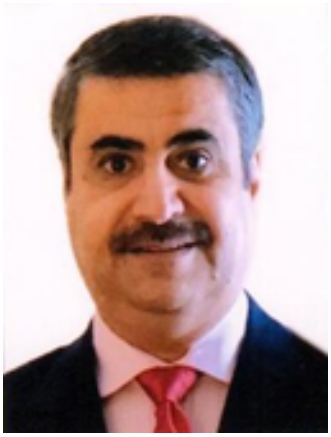
Zyber News Roundup

GLACY+: Building a solid foundation for measuring the impact of cybercrime

INTERPOL and the Council of Europe, in the framework of the GLACY+ Project, cooperate in publishing the *Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence.*
Many countries are recognizing the need to take actions against cybercrime, but they face difficulties in defining the problem at hand. To effectively tackle the multifaceted and imperceptible cybercrime, criminal justice authorities require a good and better understanding of the scale, types and impact of the crime. For this reason, the Council of Europe and INTERPOL jointly developed the *Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence* to support countries in having a clearer vision of the global problem.
The key goals of this joint effort is to help criminal justice authorities worldwide in introducing the statistics on cybercrime and electronic evidence by providing good practices and recommendations. The statistics enables the authorities to shape effective policies and operational responses. This guide lays out the agenda for compiling criminal justice statistics with key steps for data collection, analysis and cooperation among multiple stakeholders.

Read the full story: https://www.coe.int/en/web/cybercrime/-/building-a-solid-foundation-for-measuring-the-impact-of-cybercrime

Read the report: https://rm.coe.int/3148-3-1-12-guide-for-criminal-justice-statistics-on-cybercrime-and-ee/1680a0250a



Zyber Spotlight

H.E. DR. ALI BIN FADHEL AL-BUAINAIN
ATTORNEY GENERAL,
KINGDOM OF BAHRAIN

His Excellency has been innovative and progressive in responding to the ever growing threat of cybercrime. Through training, legislation and policies, he has enhanced the capabilities of the Public Prosecution Service to robustly meet the challenges of investigating and prosecuting cybercrime

Can you tell us a bit about yourself and your journey to where you are today in your career?

I started as a member of the prosecution service in 1985 before the establishment of the Public Prosecution. In 2005, I was appointed as the Attorney General of the Kingdom of Bahrain, and I am still holding this position to date.

What has been Bahrain's experience of cybercrime to date?

In general, the rate of cybercrimes committed in the Kingdom of Bahrain is limited, however, the use of electronic means often appears in committing other types of crimes.

As the Attorney General what measures have you put into place to effectively combat cybercrime?

Since I assumed the position of the Attorney General, a sustainable plan has been put in place to develop the Public Prosecution structure and to improve the capabilities of its members based on several aspects, including training on the thorough investigation of serious crimes such as terrorism, money laundering, and cyber and information related crimes, whether they are used in these criminal activities or committed independently. Prosecutors have participated in numerous training courses and seminars, the topics of which are related to information technology crimes in all their forms. They have also received training from experts in law and information technology. It is worth noting that training programs are organized continuously from time to time due to our belief in its importance, especially to keep abreast of developments in fighting crimes of such nature and applying successful experiences.

Can you tell us something about how cybercrime affects the Middle Eastern Region? Is there any regional collaboration to tackle cybercrime?

It is noticeable that a crime often appears as fraud and appropriation of funds, either directly from the victim or by hacking bank accounts. Electronic communication systems are sometimes used to commit crimes of personal injury to reputation and honor.

There is cooperation existing among all Arab countries, and between the Gulf Cooperation Council (GCC) countries, which is governed by cooperation agreements that are used as a legal basis for legal assistance requests.

For the full interview see:
https://zyberglobal.com/my-blog

Zyber News Roundup

Unveiling the cost of cybercrime in Africa

Cybercrime is one of the most pressing challenges plaguing economic activity in Africa. With poorly secured telecommunication infrastructure in many African countries, the footprint of cybercrime is exacerbating the numerous socio-economic problems in the region.

As Africa's gross domestic product (GDP) reached $3.3 trillion in 2017, the cost of cybercrimes for the same year also amounted to a total of $3.5 billion; Nigeria, Kenya and South Africa recorded the largest losses.

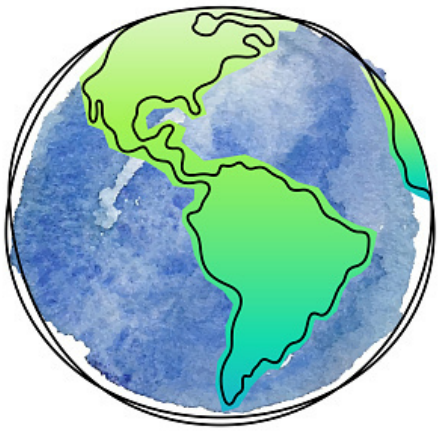
For most African countries, unsecured telecommunication infrastructure has created an enabling environment for cybercrimes to thrive; a situation which partly accounts for the decline in productivity across several sectors. It is quite surprising to note that more than 90 percent of African businesses are operating without the required cybersecurity apparatus.

Furthermore, in financial institutions, governments, e-commerce companies, mobile-based transactions, telecommunication industry and other industries, the impact of cybercrime is severe. The rapid growth in Africa's digital economy has outpaced developments in providing adequate cybersecurity for telecommunication infrastructure.

However, for most financial institutions in Africa, providing appropriate cybersecurity mechanisms to secure financial assets has been a daunting task as losses attributed to cybercrimes have increased significantly in the last few years. The findings of a recent study conducted to assess the cybersecurity environment of 148 banks in Sub-Saharan Africa (SSA) suggests that 24 percent of all cybercrimes are related to malware; credit card fraud and phishing account for 30 percent and one-third of all cybercrimes, respectively.

Read the full story:

https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html



Zyber Focus
Drugs and Cybercrime, Part 2

As the Silk Road closed having been 'shut down' by the FBI in 2013, other similar cryptomarkets emerged to fill the void. These cryptomarkets as they are known are easily accessible provided one has a normal internet connection and special anonymising software for access. However, they tend to be short-lived due to targeted operations by the police.

According to RAND (a non-profit research and development company) illegal online drug transactions have tripled since 2013 with revenues almost doubling. In 2016, it was found that the online drug trade accounted for approximately €10.5 - €18.0 million a month compared to the traditional offline market which is estimated at €2 billion a month in Europe alone.

RAND, Europe had been commissioned in 2016 by the Research and Documentation Centre (WODC) on behalf of the Dutch Ministry of Security and Justice to ascertain the scope and size of the drug trade over the internet.

Some of RAND's findings were as follows:

- There was evidence that drugs being sold on cryptomarkets were supplying offline drug markets, with buyers sourcing stock for offline distribution. Twenty five per cent of total drug transactions on cryptomarkets during January 2016 were greater than $1,000 (€877.2) (values at April 2016),which suggested that these drugs were being bought for wholesale purposes. The majority of drugs sold on cryptomarkets were under $100 (€87.7), so were more likely to be for personal use, but they only generated 18 per cent of total transactions.
- Cannabis was a best seller followed by stimulants (cocaine and amphetamines) and ecstasy type drugs.
- The vendors were from the U.S, U.K, Australia, Canada and Western Europe.

RAND also looked at Modes of Detection and Intervention. The Study identified four broad potential strategies that are available to law enforcement agencies in the detection and intervention of the internet facilitated drugs trade:

1. traditional investigation techniques applied in the drug chain (e.g. surveillance, undercover operations);
2. postal detection and interception (e.g. collaboration between law enforcement agencies and postal services);
3. online detection (e.g. big data techniques, monitoring of online marketplaces, tracking money flows); and
4. online disruption (e,g. taking down online marketplaces).

International collaboration was also found to be a highly useful and major tool in the investigation and taking down of these markets.

The 21st century has ushered in a tidal wave of technological advances that have changed the way we live, but as technology has evolved, so too have the tactics of drug traffickers.
U.S DEA Acting Administrator Timothy J. Shea.

In more recent times, (September 2020) the Department of Justice, U.S through the Joint Criminal Opioid and Darknet Enforcement (JCODE) team worked closely with EUROPOL to lead Operation DisrupTor.

This operation resulted in the seizure of over $6.5 million in both cash and virtual currencies; approximately 500 kilograms of drugs worldwide; 274 kilograms of drugs, including fentanyl, oxycodone, hydrocodone, methamphetamine, heroin, cocaine, ecstasy, MDMA, and medicine containing addictive substances in the United States; and 63 firearms.

Operation DisrupTor showed that through joint collaboration, and innovative investigations these cryptomarkets can be disrupted and shut down, despite their attempt to operate anonymously.

Zyber Global Events

Zyber Global's ***Stay Safe Online Webinar*** is on Monday 30 November 2020 at 1600 hours GMT. ***Register now to attend.***

OTHER CYBER SECURITY EVENTS

"Effective Access Electronic Evidence: Towards a new Protocol to the Budapest Convention." 9 November 2020	Virtual International Conference on Cyberlaw, Cybercrime & Cybersecurity (ICCC) 25th, 26th & 27th November, 2020	The Cyber Security & Cloud EXPO, Europe 2020 25 -26 November 2020, (Fully Virtual)
.The increased use of new technologies by criminals to organize, plan and carry out illegal activities online put the spotlight on the use of electronic evidence in criminal investigations. The latter is crucial, not only for investigating cybercrime but any type of crime. The globalization of the communication infrastructure brings additional challenges for investigators as offenders, victims and electronic evidence may be located in multiple jurisdictions and conflicting national laws may apply to obtain such evidence.	The 2020 Conference aims to examine and analyze the emerging Cyberlaw, Cybercrime and Cybersecurity trends of today's times. This conference has the distinction of being the only conference focusing on the intersection of Cyberlaw, Cybercrime & Cybersecurity.	Showcasing the next generation technologies and strategies from the world of cyber security and cloud, expand your knowledge and gain the security skills needed to steer your organisation to a more secure future. Over two days the event will showcase the most cutting-edge technologies from more than 300 exhibitors and provide insight from over 500 speakers sharing their unparalleled industry knowledge and real-life experiences.
. For further information: https://www.coe.int/en/web/cybercrime/effective-access-to-electronic-evidence-towards-a-new-protocol-to-the-budapest-convention	For further information: http://cyberlawcybercrime.com	For further information: https://cybersecuritycloudexpo.com/europe/

Zyber Global Online Events

Our Online Courses with INsig2
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/
For an extra 15% off use coupon code ZYBER
during checkout.

Courses per sectors

Legal Entities
Judges, lawyers and public prosecutors
Customized courses for legal entities on deeper aspects of digital forensics and forensic value of the evidence while collecting, processing, and presenting digital evidence in criminal and administrative proceedings. a subheading

Law Enforcement
First responders, forensic investigators and analysts
Customized courses for law enforcement officials on procedures, techniques, and tools used in digital forensic analysis and how to apply them in their forensic investigations.

Private Sector Corporations and small businesses.
Customized courses for various industry professionals working in the private sector ,to help them understand the value and the need for digital forensic, and its implications in a corporate environment.

Course Structure

- Full Text Reading
- Quiz after each chapter
- Case study final exam

At the end of each course, you will be issued a completion e-certificate which is immediately printable for your records. Certificates brings you CPD (Continuing Professional Development), CPE (Continuing Professional Education), CLE (Continuing Legal Education) points. The number of points depends on the course.

Discounts

Use the code **ZYBER** and get 15% off on your first-time purchase.
Special discount for groups of 10+ participants on all courses. The bigger the group, the bigger the discount.

Bundles

Stay on your digital forensics learning path and get the most from your e-learning experience by using course bundles. https://bit.ly/3lNRYsj

Free Courses
Password Management

The course covers different lock security methods, guidelines on securely storing your passwords, various password managers and how to use them
https://bit.ly/3eMu7FD