

Zyber Global

MAY 2023 | ISSUE 34

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to Zyber Global Centre's monthly newsletter - May 2023, the 34th edition!

April was a busy month for me but May looks like it's going to be even busier.

We have set up the Zyber Global Community it's a private global group for criminal justice authorities and other government officials where they can connect with each other, share information, best practices, and expertise which will help members to combat cybercrime.

The Community will be a place where we can improve our collective understanding of cybercrime and build a stronger and more effective response to this growing threat. We know that together we can make a real difference in the fight against cybercrime and protect our communities from these evolving threats.

You can join the community with the link below. I look forward to welcoming you to the Community.

<https://www.facebook.com/groups/zyberglobalcommunity>

I am excited to announce that we are arranging a series of 5 free online webinars. The first webinar on "Global Perspectives on Cybercrime: Challenges and Solutions," we are hosting on the 31 May 2023 at 12:00 -13:30 CEST. Further details are on page 2 of the newsletter, places are limited, so hurry up and reserve your space here

<https://www.subscribe.com/zgcwebinar>

As always, do let us know what topics you would like to see discussed in the May 2023 newsletter. Stay safe!



Esther George, CEO Zyber Global Centre

BEST REGARDS
ESTHER GEORGE



Zyber Global - Tel: 07426719579 [Privacy Policy Register](#)
To unsubscribe contact us at office@zyberglobal.com

This Month's Features

Zyber Focus Article

Zyber Global Centre hosts the first of a five part webinar series:

"Global Perspectives on Cybercrime: Challenges and Solutions," 31 May 2023 at 12:00 -13:30 CEST, Online.

Zyber News

We have a roundup of the latest international cybercrime news.

Zyber Global Events Information

A focus on forums/conferences around the world.



Gerd Altmann, Pixabay

"Most people are starting to realize that there are only two different types of companies in the world: those that have been breached and know it and those that have been breached and don't know it."

Ted Schlein, a partner at Kleiner Perkins
Caufield & Byers

Zyber Focus Article

Zyber Global Centre 1st Webinar Global Perspectives on Cybercrime: Challenges and Solutions

**Date and time: 31 May 2023 | 12:00
-13:30 CEST, Online**



Esther George
CEO, Zyber Global Centre
Facilitator and Host of the Webinar

Esther George is an independent cybercrime, cybersecurity and digital evidence consultant with over 20 years of experience in the field and is the CEO and founder of the Zyber Global Centre. Since April 2014 to present Esther has worked as a cybercrime consultant with organisations such as the Council of Europe, Commonwealth Secretariat, European Union and UNODC. Esther regularly travels abroad to train judges, prosecutors and law enforcement on cybercrime, electronic evidence and international cooperation. Esther is also the Lead Cybercrime Consultant for the Global Prosecutors E-Crime Network (GPEN) which is part of the International Association of Prosecutors. Additionally, Esther has authored several published papers on topics such as digital evidence and cloud computing, and obtaining evidence from mobile devices.



Ana Gogovska Jakimovska
Prosecutor, Public Prosecutor's Office, North Macedonia
Topic: "Lessons Learned: What Cybercrime Prosecutors Wish They Knew from the Start."

After graduating from the Faculty of Law in Skopje, St. Cyril and Methodius University, Ms Jakimovska obtained a masters degree in intellectual property rights protection from the Faculty of Law in Skopje and the Faculty of Strasbourg, France. In 2016, she was appointed as a Public prosecutor in the Basic Public Prosecution office in Skopje, where she continues to work till today. Ms Jakimovska specialises in cybercrime offences, human rights offences, financial investigation, abuse of official position and authority. From 2019, she has been an integral part of the national team for cybercrime and work on several projects for capacity building.



Matteo Luchetti
Director of CYBER 4.0, the National Cybersecurity Competence Center, Italy
Topic "Cybercrime in Europe: Challenges and Solutions."

Matteo Lucchetti is Director of CYBER 4.0, the national Cybersecurity Competence Center promoted and cofounded by the Italian Ministry of Enterprises and Made in Italy – a public-private partnership aimed at strengthening cybersecurity capacities of Public Administration and private sector through training, advisory, research and innovation. Matteo is an Advisory Board member at the Global Forum for Cyber Expertise and an individual expert for ENISA, EU CyberNet and other international capacity building initiatives. Between 2016 and 2021 he has been Programme Manager at Council of Europe, in charge of the Global Action on Cybercrime (GLACY+), an international capacity building initiative to support criminal justice authorities worldwide to fight cybercrime. Prior to that, he worked as cybersecurity professional at the EU Fundamental Rights Agency and in the Italian financial sector. Matteo holds a PhD Systems Engineering and MSc Electronic Engineering from Sapienza University of Rome, and a MSc Cybersecurity from the Royal Holloway University of London.



D Nalon Kaine
Manager – Ministry of Posts and Telecommunications, Republic of Liberia
Topic "The Hidden Menace of Cybercrime in Africa."

D Nalon Kaine, a Liberian who has many years of working in the area of ICT. Nearly ten (10) of these years were directly related to cybersecurity experience. He is now the Manager of the Project Management Office and Cybersecurity Coordinator with the Ministry of Posts and Telecommunications, Republic of Liberia.

He was one of the main leads in drafting Liberia's first Cyber Crime Act of 2021. He is a member of the ECOWAS Regional Cybersecurity Technical Committee which produced the first Regional Cybersecurity Strategy and a Regional Critical Infrastructure Policy for the ECOWAS region. He is also serving as Focus Person to the African Union on Cybersecurity and member of the African Cybersecurity Experts (ACE).



Musa Jalloh
Deputy Director, National Communications Authority, Sierra Leone
Topic "Managing Cyber Threats to African Critical Infrastructure."

Musa Jalloh is a Retired Captain from the Republic of Sierra Leone Armed Forces. He lives in Freetown, the capital city of Sierra Leone. He has a Bachelor's degree in Information Systems from the University of Sierra Leone. After graduating with a Master's degree in Information Systems from Stratford University, New Delhi campus in December 2014, he began his career in the field of Information Communication Technology. Mr Jalloh is a member of the Africa Cyber Expert (ACE) Community and is also a member of Working Group C on Cybercrime of the Global Forum of Cyber Expertise. He has kept abreast of knowledge in the field by attending workshops, training, and seminars on Cybersecurity. He was an integral part of the team that developed the Cybersecurity Strategy for Sierra Leone and also validate the Cybersecurity and Cybercrime Act 2021.

This webinar brings together expert speakers on topics specific to cybercrime and cyber security. From the public to the private and also looking at how some African countries are responding to the growing menace of cybercrime.

The purpose of this series of thematic webinars is to increase awareness and understanding of cybercrime trends and emerging threats. To exchange views and experiences, share good practice and collaboration with others globally.

The widespread use of Information Communication Technology has led to an increase in illegal activities committed against computer systems, highlighting the need for the retrieval of evidence in criminal investigations.

Cybercrime has become more and more accessible to a wider range of individuals due to the availability of ready-made malicious software and online cybercrime-for-hire services, leading to the exploitation of new technologies for unlawful purposes.

Cybercrime affects individuals through scams, online child sexual exploitation, and cyberbullying, while organizations face threats to financial institutions and the theft of sensitive information.

We find ourselves having to be creative and develop new measures which are required to keep pace with these threats, including technical solutions to deal with encryption technologies and the complexities of transnational criminal activities in cyberspace.

Do attend this free online webinar. You can ask questions of the experts. You can make contacts, network and share good practice with those in the same field.

Register here:
<https://www.subscribepage.com/zgcwebinar>



Zyber News Roundup

South Korea, US agree to cooperate on cybersecurity and combating North Korean digital heists

South Korea and the U.S. have announced their intention to sign a cybersecurity cooperation agreement, in response to concerns about North Korea's funding of its weapons programs through cybercrime. The two allies plan to establish a "Strategic Cybersecurity Cooperation Framework," working together to deter cyber adversaries, secure critical infrastructure, combat cybercrime, and secure cryptocurrency and blockchain applications. The agreement comes after South Korean President Yoon Suk Yeol's visit to the White House, where he and U.S. President Joe Biden discussed North Korea's cyber activities and committed to blocking its cyber-enabled revenue generation.

North Korea has long relied on its government-backed hacking groups to fund its weapons programs, launching audacious attacks on cryptocurrency exchanges and medical facilities. The Lazarus Group was behind a \$100 million theft from the blockchain platform Horizon and the largest cryptocurrency theft on record, a \$625 million heist of the Ronin Network blockchain last year. The agreement is expected to extend the countries' longstanding defense pact to the digital sphere, as well as to space.

Read more:

<https://therecord.media/south-korea-us-agree-to-cooperate-cybersecurity-north-korea>

Read more:

<https://www.businessleader.co.uk/uk-highest-cybercrime-density-worldwide-last-year/>

DataFocus 2023: Connecting the Digital Forensics Community

DataFocus is an international conference, that has been successfully organized by INsig2, every year since 2012. It has been attended by more than 200 participants each year, from throughout the whole world. This year, the conference took place on 21st of March in Hilton Garden Inn Zagreb and, as every year, the goal was to bring together law enforcement investigators, prosecutors, judges, court expert witnesses and let them talk about their experiences with digital evidence and digital forensic investigations.

The conference was divided into investigation section, technical section, and workshops. It featured a variety of keynote speakers, panel discussions, exhibitors, and presentations. Attendees had the opportunity to learn from industry leaders, network with their peers, and gain valuable insights into the latest trends and technologies in the field.

It was an incredible experience bringing together so many talented professionals from the industry to share their insights and expertise on the latest trends and innovations in digital forensics and data science.

Since its beginnings, DataFocus has always been a conference free of charge for all the attendees, based on invitation of the organizer. It was and still is, INsig2's way of contributing to the digital forensics community by bringing all experts dealing with digital evidence in one place and giving them a chance to learn from one another.

Read more:

<https://insig2.com/en/conference/datafocus-2023>

New research finds UK had highest cybercrime density worldwide last year

The UK has the highest density of cybercrime victims per one million internet users, with 4371, according to a study by Surfshark. However, there was an 8.6% decrease from 2021. The US ranked second with 1612 victims, and Canada was third with 156 victims. The study found phishing to be the most common cybercrime, with 300,000 victims globally in 2022, followed by online payment fraud, extortion, tech support scams, and investment fraud. Investment fraud caused the most financial losses, amounting to \$3.3 billion in 2022.

Surfshark's study revealed that the UK is second in the world by total cybercrime count with 284,000 total cybercrime victims, surpassed only by the US with 479,000 victims. While phishing remains the most common cybercrime, investment fraud caused the most financial losses, with \$3.3 billion in losses in 2022. Cybercriminals have stolen \$36.4 billion since 2001, and yearly losses have been on an upward trend throughout this whole period.



Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

<p>Cyber Intelligence Africa</p> <p>Sandton, South Africa</p> <p>16 - 17 May 2023</p>	<p>44th IEEE Symposium on Security and Privacy</p> <p>San Francisco, CA. USA</p> <p>22- 25 May 2023</p>	<p>Zyber Global Centre Webinar Global Perspectives on Cybercrime: Challenges and Solutions</p> <p>31 May 2023</p> <p>12:00 - 13:30 CEST, Online</p>
<p>Cyber Intelligence Africa will bring together government agencies from across Africa to discuss national cyber security strategies, policies, development, and challenges faced.</p> <p>During the event, you will hear from leading government officials who are directly involved in implementing national cyber security programs.</p> <p>You will also hear of recent cybercrimes faced across the continent and response procedures to these attacks.</p>	<p>The IEEE Symposium on Security and Privacy is a forum for presenting developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field. The 2023 Symposium will mark the 44th annual meeting of this conference.</p>	<p>Zyber Global Centre presents the first of a free online 5-part webinar series organised by the Zyber Global Centre to collaborate with individuals globally, exchange views and experiences, and share good practices to foster mutual learning and growth.</p> <p>Cybercrime and cybersecurity are a growing concern for law enforcement agencies around the world. Criminals are increasingly turning to the internet to commit crimes, and law enforcement agencies must adapt to this new reality.</p> <p>We believe that by working together, law enforcement agencies and other government officials can connect with each other, share information, best practices, and expertise which will help them to effectively combat cybercrime.</p>
<p><u>For further information</u></p> <p><u>https://10times.com/e1z3-p6z0-r2kr</u></p>	<p><u>For further information</u></p> <p><u>https://www.ieee-security.org/TC/SP2023/</u></p>	<p><u>For further information</u></p> <p><u>https://www.subscribepage.com/zgcwebinar</u></p>



Zyber Global Online Events

Our Online Courses with INsig2

Sign up now at <https://insig2-and-zyberglobal.learnworlds.com/>

Special discount: 15% Use Code: zyber

Courses per sectors



Legal Entities

Customized courses for legal entities: judges, lawyers and public prosecutors.

Explore deeper aspects of digital forensics and the forensic value of evidence while collecting, processing, and presenting digital evidence in criminal and administrative proceedings.



Law Enforcement

Customized courses for law enforcement officials: First responders, forensic investigators and analysts. Delve into procedures, techniques, and tools used in digital forensic analysis and how to apply them in forensic investigations.



Private Sector Corporations and Small Businesses.

Customized courses for 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 REVISION**

***QUIZ AFTER EACH CHAPTER**

***CASE-STUDY AFTER FINAL EXAM**

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

DISCOUNTS

Special discount for groups of 10+ participants on all courses. The bigger the group, the bigger the discount.

BUNDLES

Stay on your forensic digital learning path and get the most from your e-learning experience by using course bundles.

<https://bit.ly/31NRYsj>

FREE COURSE ON PASSWORD MANAGEMENT

This covers different lock security methods, guidelines on securely storing your passwords, various password managers and how to use them.

<https://bit.ly/3eMu7ED>



Zyber Global - Tel: 07426719579 [Privacy Policy](#) [Register](#)
To unsubscribe contact us at office@zyberglobal.com