Zyber Global

DECEMBER 2021 | ISSUE 17

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 17th Edition, December 2021 of Zyber Global Centre's monthly newsletter.

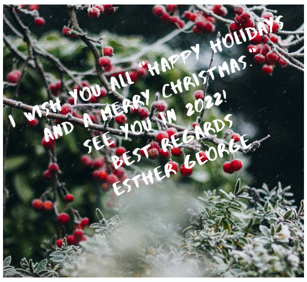
In the northern hemisphere, at this time of the year it gets dark early and it is very cold. In the UK, the weather does not disappoint! It's usually dark by four pm and we have been having snow and ice warnings in the wake of Storm Arwen. Some areas in the north of the country have been snowed in.

Whenever I am feeling down because of the weather, I just remind myself that a couple of weeks ago I was happily enjoying the lovely sunny weather in Liberia. I look at my favourite beach scene (see photo below) from my time in Liberia and happily remember sun, sea and sand. I was honoured to be working in Liberia with Expertise France, The Liberian Government and ECOWAS (Economic Community of West Africa) to train judges and prosecutors on cybercrime. I was training a great group of delegates who were very committed to the training, so much so that one of the training days was a public holiday and all the delegates still turned up for the training on time. I was very impressed!

December is the month of holidays which is why it's called the festival season. I am looking forward to celebrating Christmas I am as usual not sending Christmas cards but rather I have given a donation to three charities that are close to my heart as I am in awe of the work they do.

This year the three charities are:
***Campbell Village Trust** - https://www.camphillvillagetrust.org.uk They help people live independently who have learning difficulties or mental health challenges.*
***Compassion UK** - https://www.compassionuk.org They are releasing children from poverty all over the world. My last charity is the **Salvation Army**, https://www.salvationarmy.org.uk the Salvation Army (as they are all year round) will be there for people who are lonely, desperate, homeless or hungry this Christmas.*

As always, do write in and let us know what topics you would like to see in the New Year. This is your newsletter and we always appreciate your feedback! In the meantime, keep safe!!



Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Spotlight

The interview spotlight this month is on General Eric Freyssinet, Deputy Commander of the Gendarmerie Nationale's Cyberspace Command, France.

Zyber News

We have a roundup of the latest international cybercrime news.

Zyber Global Events

The next Stay Safe Online Webinar by Zyber Global is due to take place on Thursday, 27th January, 2022 register now to attend.

> ***"We need to keep improving our cooperation tools and for instance very quickly implement the second protocol to the Council of Europe Budapest Convention on Cybercrime, to be adopted this November 2021. It brings us many practical legal solutions addressing concerns with prompt access to digital evidence and judicial and police cooperation. "***
>
> ***GENERAL ERIC FREYSSINET***
> ***DEPUTY COMMANDER***
> ***GENDARMERIE NATIONALE'S CYBERSPACE COMMAND, FRANCE.***

Zyber Spotlight

GENERAL ERIC FREYSSINET

Deputy Commander of the Gendarmerie Nationale's Cyberspace Command, FRANCE

Can you tell us about yourself and your journey to where you are today?
After graduating from the Ecole Polytechnique in 1995, I joined the *Gendarmerie Nationale* and very quickly was attracted to our national forensic lab in 1998. Since then, I have been "growing up" at the same time as the gendarmerie was developing its response to cybercrime. In parallel, I have had the chance to keep developing my knowledge in an academic framework and defended a PhD in computer science on the topic of the fight against botnets in 2015.

What interested you about cybercrime?
My first interest was personal, as an early adopter of digital technologies and having discovered the Internet in 1993. I had also quickly discovered its potential abuses. But what drove me most was the capacity of the *Gendarmerie Nationale* to embrace new technologies and new challenges, serving the public.
The challenge is both technical and human. Human, through the need to train the law enforcement officers but also in contact with the victims and the growing community of digital evidence and cybercrime fighting specialists over the year.

What is the best part of your job?
From the beginning, I have been driven by the technical challenges and the richness of human exchange. The most exciting moments for me are when collectively, as a team, we have a technical or investigative breakthrough, helping solve a case and arrest criminals.

What cybercrime training is provided for French law enforcement officials?
There are several course tracks for gendarmes to be trained against cybercrime. It all starts at the very first steps and the initial training. Every law enforcement officer must have a basic understanding of cybercrime and act properly as a first responder. Then, the gendarmerie offers specialised training for specialised investigators: C-NTECH (local digital crime correspondent), NTECH (specialised cybercrime investigator), FINTECH, online covert investigators (ESP).
These training tracks are the product of a dense partnership policy between the gendarmerie and associated university (Université Technologique de Troyes, Université de Bretagne Sud), that offer dedicated courses for selected investigators of the Gendarmerie.
Finally, the creation of the ComCyberGend incarnates the will of the Gendarmerie to attract more people with scientific backgrounds, and will provide support to the creation of e-companies where the proportion of basic teachings about cybercrime and security are increased (from 8% of the training time to ~40%).

What mechanisms are in place in France to track cybercrime?
Our first source of information is the victim themselves that can report crime through online platforms or by filing a formal complaint. We are constantly improving that process, in particular when dealing with ransomware cases, where a fast response of law enforcement is key to be able to collect evidence at the source and give proper advice to the victims.
Our second method for tracking cybercrime is through targeted monitoring of illegal online activities, with the capacity, if needed to enter into a formal covert investigation – using a pseudonym, to gather more evidence and identify the criminals behind the suspicious activity.
And of course we also develop communication channels with private actors and OSINT communities in France and around the world. We have lots of hope in a new initiative that will bring many CERTs, academia and other cybersecurity specialists together in the same building next year, called the Cyber Campus. We are thrilled to be part of that adventure and part of its activities will be about sharing information on cyberthreats.
Read more: https://zyberglobal.com/my-blog

Zyber News Roundup

DR Congo data leak: Millions transferred to Joseph Kabila allies

Companies owned by family and friends of former Democratic Republic of Congo President Joseph Kabila had millions of dollars of public funds funneled through their bank accounts, according to Africa's biggest data leak.

The money was transferred to the companies' accounts at the Congolese arm of the BGFI bank. Millions of dollars in cash were then taken out of the accounts. Mr Kabila was president at the time of the bank transfers. In a statement published online, he called the reports "unfounded accusations".

The leak included more than three million documents and information on millions of transactions from the BGFI (Banque Gabonaise et Française Internationale) bank, which works in several African countries and France. Online French investigative journal Mediapart and the NGO Platform to Protect Whistleblowers in Africa (PPLAAF) obtained the information. BBC Africa Eye had access to the evidence, as part of a consortium called Congo Hold-up, co-ordinated by the media network European Investigative Collaborations (EIC).

The investigation raises questions about who benefitted from the money transfers and possible conflicts of interests.

The managing director of BGFI's DR Congo subsidiary, BGFI Banque RDC, from 2012 to 2018 was Francis Selemani, Joseph Kabila's foster-brother. Mr Kabila's sister, Gloria Mteyu, owned 40% of BGFI's DR Congo operation, which was set up in 2010.

One privately owned company, Sud Oil, was shown to have received nearly $86m in public funds from November 2013 to August 2017. The BBC found no evidence Sud Oil was trading in petroleum products at the time. Mr. Selemani's wife, Aneth Lutale, owned 80% of Sud Oil and Mrs. Mteyu owned the remaining 20% from 2013 to 2018.

Millions of dollars were transferred out of Sud Oil's BGFI accounts to other private companies' BGFI accounts. Some of these were owned by relatives or business associates of Mr. Kabila, who was president from 2001-2019.

BBC Africa Eye's investigation will be available online to watch from 29 November.

Read more:
https://www.bbc.co.uk/news/world-africa-59343922

Tech CEO Pleads to Wire Fraud in IP Address Scheme

The CEO of a South Carolina technology firm has pleaded guilty to 20 counts of wire fraud in connection with an elaborate network of phony companies set up to obtain more than 735,000 Internet Protocol (IP) addresses from the nonprofit organization that leases the digital real estate to entities in North America.

In 2018, the American Registry for Internet Numbers (ARIN), which oversees IP addresses assigned to entities in the U.S., Canada, and parts of the Caribbean, notified Charleston, S.C. based Micfo LLC that it intended to revoke 735,000 addresses.
ARIN said they wanted the addresses back because the company and its owner — 38-year-old Amir Golestan — had obtained them under false pretences.
A global shortage of IPv4 addresses has massively driven up the price of these resources over the years:

At the time of this dispute, a single IP address could fetch between $15 and $25 on the open market.
Micfo responded by suing ARIN to try to stop the IP address seizure. Ultimately, ARIN and Micfo settled the dispute in arbitration, with Micfo returning most of the addresses that it hadn't already sold.
But the legal tussle caught the attention of South Carolina U.S. Attorney Sherri Lydon, who in May 2019 filed criminal wire fraud charges against Golestan, alleging he'd orchestrated a network of shell companies and fake identities to prevent ARIN from knowing the addresses were all going to the same buyer.

Read more:
https://krebsonsecurity.com/2021/11/tech-ceo-pleads-to-wire-fraud-in-ip-address-scheme/

North Korean Hacking Group Targets Diplomats, Forgoes Malware

North Korean cyber-operations group has increased its focus on cyber espionage and targeting diplomats and regional experts, using captured user credentials to fuel phishing attacks and only rarely using malware to persist in targeted organizations.

A new report by message-security firm Proofpoint, which focused on a single subgroup of what other security firms call Kimsuky, found that the North Korean group mainly targets individuals in the United States, Russia, and China, and usually attempts to quietly harvest credentials, siphon off information, and — like many attacks attributed to North Korea — turn compromises into financial gain.

Read more: https://www.darkreading.com/threat-intelligence/north-korean-groups-focus-on-financial-gain-persistence

Zyber Global Events

The next **Stay Safe Online Webinar** by Zyber Global is due to take place on Thursday, January 27, 2021. Register now to attend.

OTHER CYBERSECURITY EVENTS

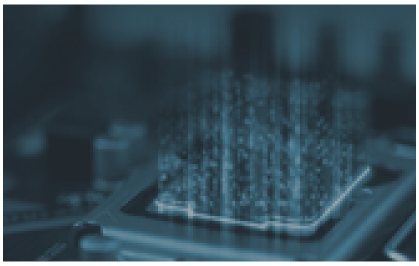
IAP & COUNCIL OF EUROPE SERIES OF WEBINARS: “SECOND ADDITIONAL PROTOCOL TO THE CONVENTION ON CYBERCRIME ON ENHANCED COOPERATION AND DISCLORE OF ELECTRONIC EVIDENCE" **7th of December at 15.00 Central European Time.**	**EAI ICDF2C 2021 - 12th EAI International Conference on Digital Forensics & Cyber Crime Singapore** **December 7- 9, 2021,**	**International Conference on Cyber Defense and Security Information London, United Kingdom** **December 9-10, 2021**
This webinar underlines the need for effective criminal justice action, making use of frameworks such as the Budapest Convention on Cybercrime and additional solutions, including those being developed for the 2nd Additional Protocol[1]to permit instant cooperation in urgent and emergency situations subject to human rights and rule of law safeguards. The third thematic webinar on 7th of December 2021 will focus specifically on the new procedures for giving effect to orders from another party for expedited production of subscriber information and traffic data, as foreseen in the 2nd Additional Protocol to the Budapest Convention. Registrations are now open for the webinar. In order to participate please register before 6 December 2021, 15h00 CET. We strongly recommend to register as soon as possible, using your professional email address, if possible. The webinar will be held in Engllsh and the discussion will be recorded. .	The focus of this year’s conference is on various applications of digital evidence and forensics beyond “traditional” cybercrime investigations and litigation. Topics may include new challenges posed by emerging technologies, including 5G, edge computing, AI-controlled systems, cryptocurrencies, darknet investigations, hardware forensics, and AI-based systems to process unstructured information such as CCTV, social media, IoT data. This year, quantum computing is being added as a current topic. Potential workshops may include password cracking for forensics, forensic education, forensic applications of AI (e.g., AI for network detection), responding to an incident from a police or corporate interaction perspective, including what to expect when you involve law enforcement.	The International Conference on Cyber Defense and Security Information aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cyber Defense and Security Information. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Cyber Defense and Security Information
For further information: https://primetime.bluejeans.com/a2m/register/ztpygeuh	For further information: https://icdf2c.eai-conferences.org/2021/	For further information: https://waset.org/cyber-defense-and-security-information-conference-in-december-2021-in-london

Zyber Global Online Events

Our Online Courses with INsig2
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/

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**

c

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