

Dr Audrey Guinchard, University of Essex

 abguin@essex.ac.uk

The criminalisation of cybercrime.

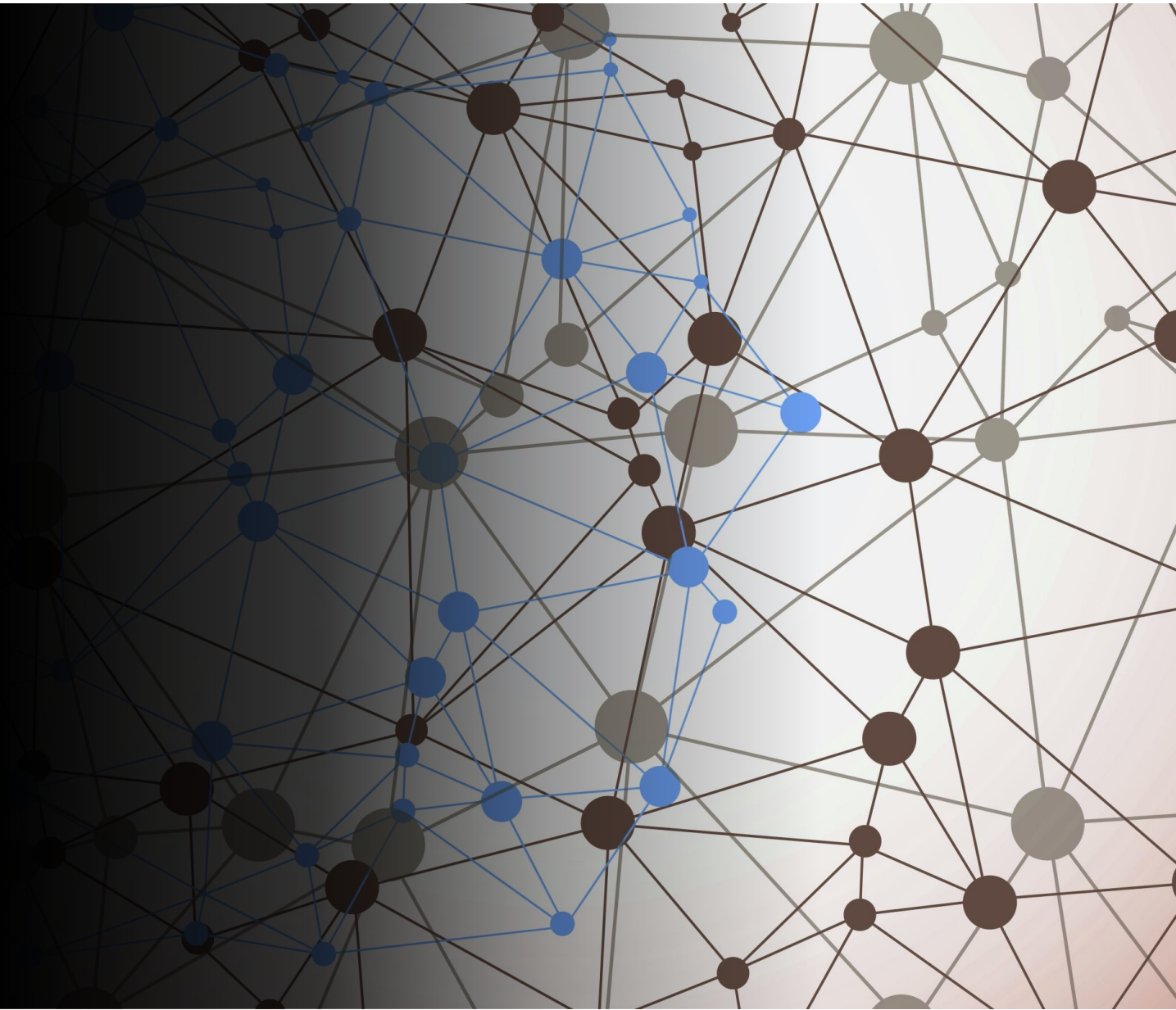
Connected dots and blind spots
in the development of legal
instruments.





Outline

- Background to/scope of this embryonic research project
- Part I: connected dots
- Part II: blind spots
- Conclusions

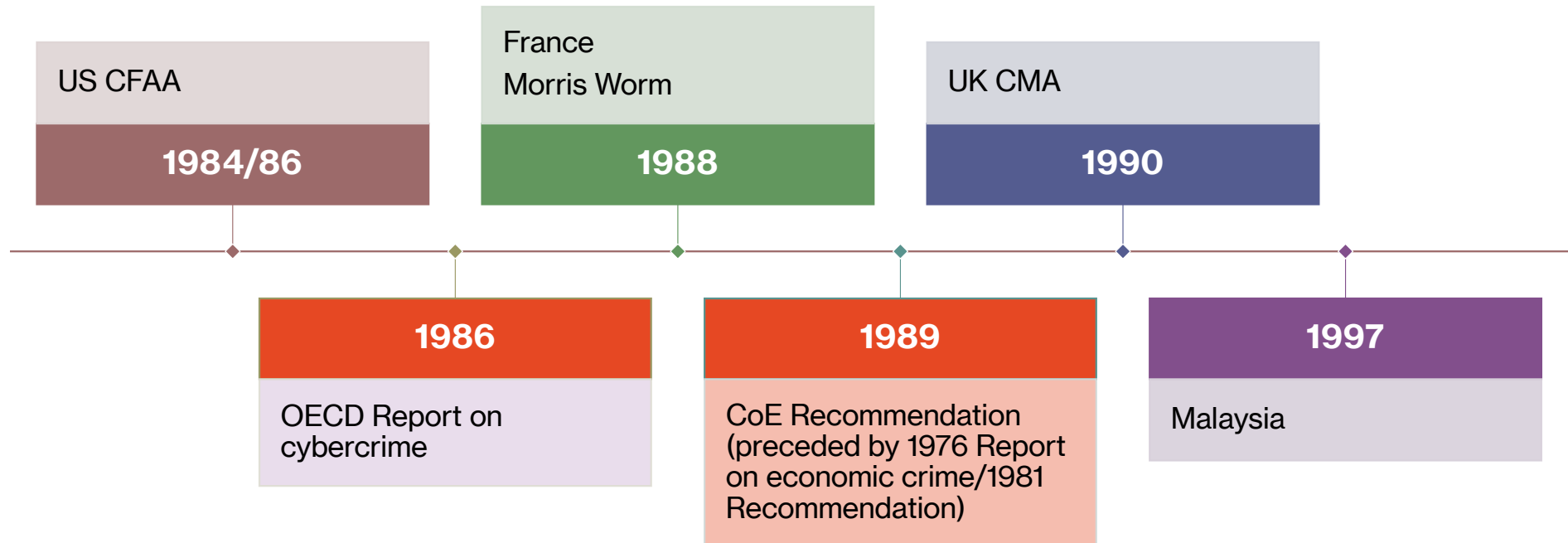


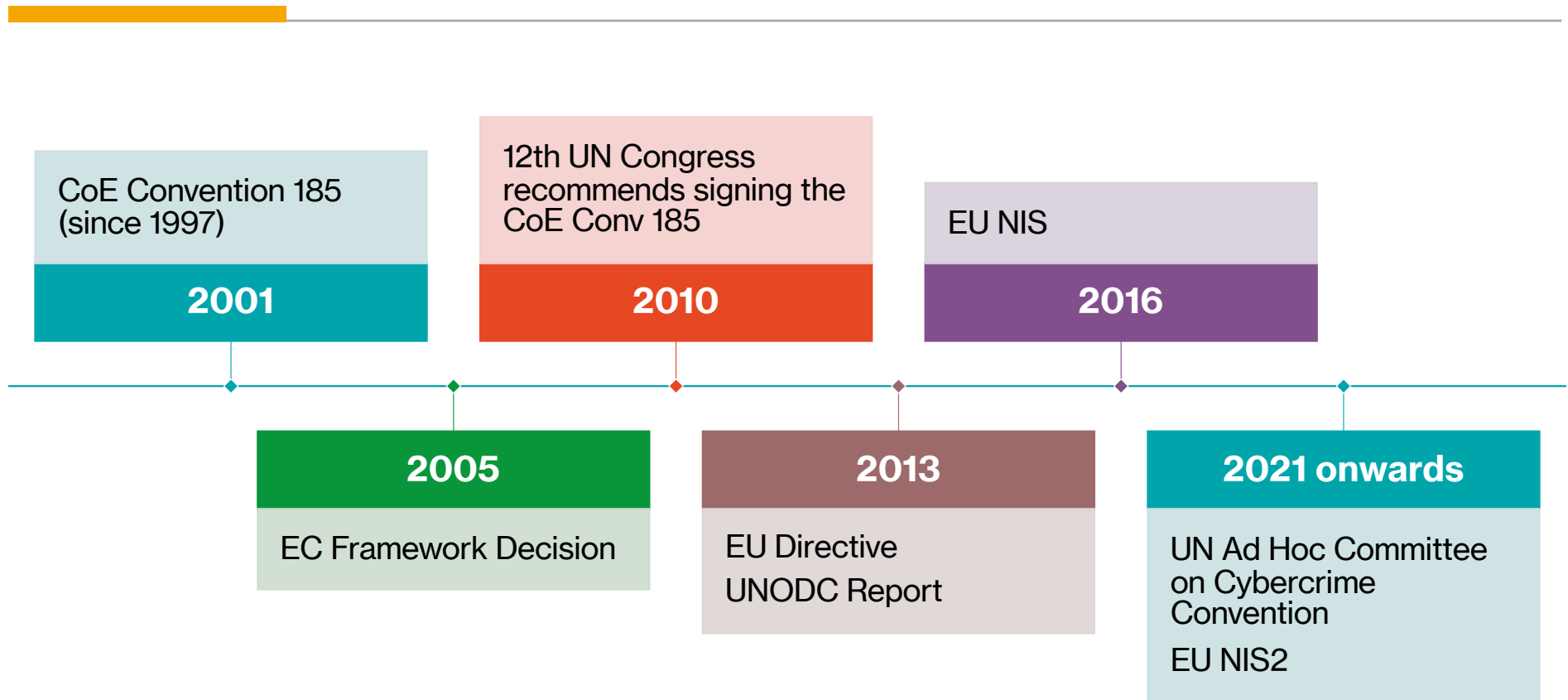


Scope

- Computer-focused crimes only
 - Unauthorised access
 - Unauthorised damage and interference (malwares; DDOS)
 - Misuse of tools

Timeline of legal instruments





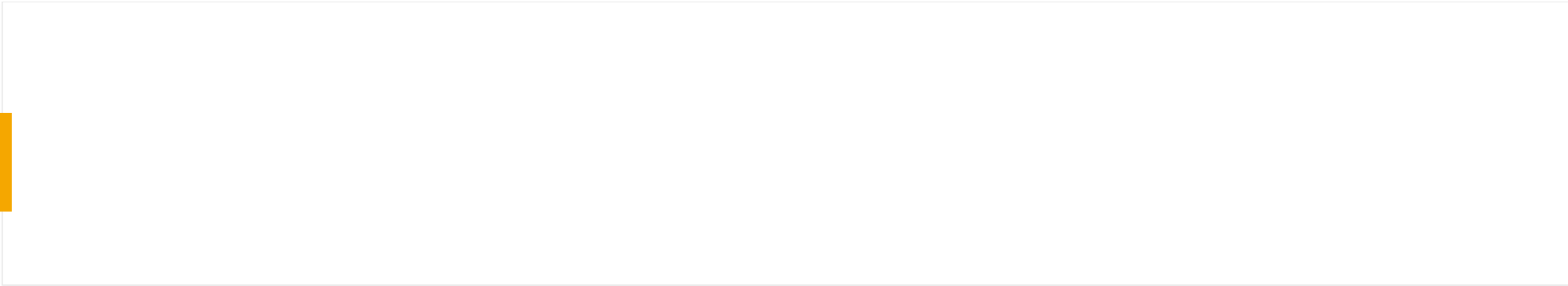
Background work

- Work on the unwarranted criminalisation of certain groups:
 - proposal of defences for security researchers and journalists/whistle-blowers
 - Had to review how the offences above were created
 - Had to integrate the current discussions on the draft UN Convention on cybercrime
- => patterns emerge



Connected dots

- The origins of cybercrime legislation: the influence of the scientific community on the law
 - [Donn Parker](#) (computer science) & August Bequai (US Lawyer) for US CFAA
 - A Bequai drafts the CoE 1989 Report/Recommendation ([ACM profile](#))
 - Scientific community (CoE 2001):
 - 1999 created CVE (Common Vulnerabilities Exposure) board, in October 2000 includes US and UK computer scientists
 - [Dorothy Denning](#) (Autumn 2000)
 - Peter Sommer (UK)

- 
- What did they achieve? Narrowing the scope of criminalisation of future Article 6 CoE (misuse of tools) in 4 different ways:
 - Restrict tools to those primarily created and adapted for cybercrime purposes
 - Intent
 - Possession vs production/sale/distribution
 - Article 6(2) = reserve of interpretation by courts
 - Indirect influence on the law through work on cybersecurity:
 - give feedback to international & regional organisations looking at cybersecurity, notably vulnerability disclosure and markets (ENISA which looked at China, US, Japan; OECD)
 - EU NIS 2

Connected dots

- The technology of the internet itself is the result of international collaboration between US (Vint Cerf; Bob Kahn), UK (Tom Berner-Lee at CERN) and France (Cyclades project with Louis Pouzin) as main countries,
 - but with a twist: the US protocol TCP/IP won over X.25 (IUT, Russia, France, lots of African countries)
- Massive undertaking of the UNODC with its 2013 report: big comparison
- Massive influence of the CoE 185 ratified by 67 states (so beyond the 48/47 Member States) in Africa, Latin America, Australasia, and Asia



This Photo by Unknown Author is licensed under [CC BY-ND](#)

Blind spots – vulnerabilities are doors to cybercrime

- Cybercrime as computer-focused crime mostly stems from poor cybersecurity standards.
 - Not a coincidence that the CoE named these Title 1 offences not 'cybercrime offences' but 'offences against the CIA of computer data and systems'
- Security is not just a technical standard: it has HR implications-civil society implications (Pegasus software)

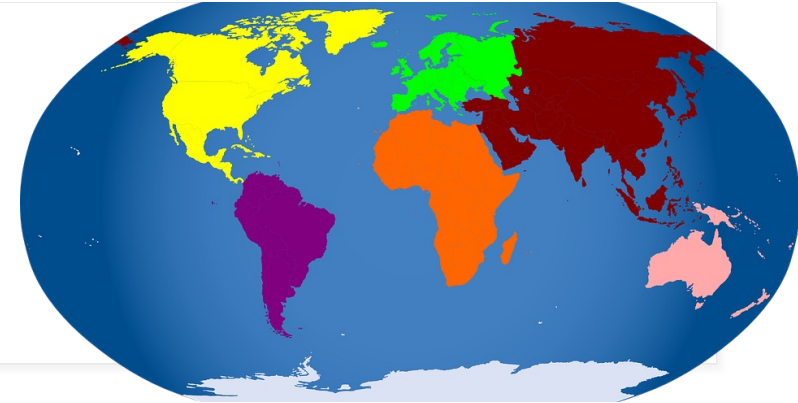


This Photo by Unknown Author is licensed under [CC BY-SA](#)

The legal environment/institutions roughly ignore/s what this entails

- Implementation of Article 6 CoE and Article 7 Directive is appallingly poor – only one legislation provides a reliable defence
- Absence of an international legal protection against Articles 2, 4 and 5 CoE / Art 3, 5 & 4 Directive – id. At national level (unless prosecutorial guidance or partial waiver of liability as in France through CERTs)
- UNODC 2013 report does not look at the interaction between cybercrime criminalisation and cybersecurity (no questions)
- UN Ad Hoc Committee: some (partial) hope with the first question drafted for the second session **but** big disappointment in terms of national responses (complete sidelining of the question)

Blind spots – non-Western voices



- Because the tech initially originates from the US + Internet TCP/IP protocol won the battle, dominant voices have been from the West
 - With a few outliers as observers: Japan (OECD + CoE 185); South Africa (CoE 185)
 - ? Dominance of anglophone ?
- Progressively**, other voices emerge, but dominance of CoE 185:
 - Commonwealth Model Law 2002 [concomitant](#) to CoE 185 and based on a late CoE draft
 - COMESA Cybercrime Model Bill 2011 (Common market for Eastern and Southern Africa)
 - African Union 2014 (Malabo) [Convention](#) on Cyber Security and Personal Data Protection (third Part) – but 13 ratifications for 55 countries; compare with 4 ratifications of the CoE 185 which do not always overlap with the AU Convention
 - But the Organization of American States (OAS - intergovernmental) recommends signing CoE 185 since 2004

** thanks to my Ethiopian PhD student [Molalign Asmare](#) for this information

UN Ad Hoc Committee 2021

- Three sessions: first on definitions/scope; second on offences; third on procedure
- Submissions to the second session: see https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html
 - By multi-stakeholders: dominance of western originated organisations (HRW, Article 19, ICC, Interpol, Microsoft, Chattam House, EFF); DP Brasil Research Association and Derechos Digitales are roughly the exceptions
 - For countries, more balanced representations, although geographically speaking, West still dominates.




This Photo by Unknown Author is licensed under [CC-BY-SA-NC](#)

Europe /West	Africa	South America	Carribean	Asia	Middle East
UK	Angola	Argentina	Jamaica - CARICOM	India	Iran
EU	Burundi (with Russia also)	Brazil	Dominican Republican	Japan	Jordan
Switzerland		Colombia		Malaysia	
Norway	Egypt	El Salvador		Singapore	
US	Ghana	Mexico		Vietnam	
NZ	South Africa	Urugay			
Australia	Tanzania	Venezuela			
Canada					
Russia	Burundi (via Russia)	Nicaragua (via Russia)		China (via Russia)	
Belarus (via Russia)				Tajikistan (via Russia)	



Blind spots - stats

Official stats on cybercrime are often poor;
multiple reasons (poor reporting; tools for 'physical' crimes, not online;
confusion with other offences such as fraud and other economic crimes)



Why does this matter?

- Computer-focused crimes are by their nature different from computer-enhanced crimes;
 - Dogma of the offline-online consistency; the motus operandi of unauthorised access (hacking) has no equivalent offline; that of fraud offline and phishing is structured along the same lines (a lie –often based on half-truths- to obtain information and money)
 - Yet, regulation is often sought for both concomitantly even though we could argue that the differences warrant separate responses
- Computer-focused crimes mostly exploit vulnerabilities – yet the impact on the cybersecurity community barely registers with the legal community
 - Cybersecurity regulations are likely to be weakened in their impact if the law does not follow or lead the way

- Digital divide: countries left on the margins with poor cybersecurity community which in turn facilitates cybercrime; the response to cybercrime usually ignores the above points
- Paucity of information on implementing the law =
 - difficult to quantify whether legislation is useful
 - Leaves grey areas

Villes africaines, comment concilier développement durable, modernisation et innovation ?

ciomag LA REVUE DU MANAGEMENT EN AFRIQUE

Jeudi 6 Octobre 2022

Hôtel Hyatt Regency - Casablanca (Maroc)

 Digital AfricanTour

ciomag **CIO MAG** 8,591 followers 1d •

Hackers Sans Frontières et **YesWeHack** : s'engagent ensemble pour protéger les ONG 🙌

Ce partenariat stratégique intervient dans un contexte de **#digitalisation** exponentielle du continent africain.

A l'ère de la révolution **#numérique**, les opportunités se multiplient, les cyber menaces aussi : il est essentiel de protéger les plus vulnérables et de former la jeunesse face à ces enjeux 🧑🏫

https://lnkd.in/eXrH_tzp

Edith Brou Bleu Lacina Koné Karim LAMOURI Clément Domingo Jeannie Cointre Guillaume Vassault-Houlière Rodolphe Harand Romain LECOEUVE Vincent Subilia

[See translation](#)

Conclusions?



And the Answer is...

[This Photo](#) by Unknown Author is licensed under [CC BY](#)

- Not sure there is any!!
 - Or it may be the chicken and egg dilemma
- If our starting point is the protection of the cybersecurity community, we see that proposing a defence to cybercrime laws would imply a wider range of reforms:
 - An obligation to acknowledge their role and build a regulatory framework alongside cybercrime legislations (recognition of expertise; standards..)
 - The need for the legal profession to specialise in computer science (and the reverse would also be true, at least beyond a bare exposure to ethics)
 - The need for Governments to acknowledge their role in finding and exploiting vulnerabilities for defence purposes
 - -> the need to regulate their involvement -> politically unsavoury?

- If we expand on this and see security not as a technical standard, but as a tool to safeguard human rights (privacy, freedom of expression) and civil society, we touch on another dimension also politically unsavoury including in the West (Assange in UK/US).
- Cybercrime legislations, when questioned, reveal the traditional fault lines of criminal law – is criminal law an instrument of oppression or of balanced regulation of crime viewed as fostering a certain type of civil society?
- The discourse and general acknowledgement of the transborder nature of cybercrime masks these tensions.

