

Comments on the proposed Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Prepared by Angus M. Marshall, n-gate ltd., 14th June 2022

Introduction

These comments are made in my capacity as an independent digital evidence investigator, advisor to law-enforcement agencies, expert witness, associate editor of a relevant research journal, editor of relevant international standards and a researcher in the field of digital forensics and the application of quality standards in digital forensic investigations.

Comments and suggestions on the themes of International Cooperation, Technical Assistance and Mechanism of Implementation

I thank you for your attention, and for the excellent progress which has been made. It was a pleasure to observe the sessions and hear the contributions from all parties. I congratulate the AHC, the secretariat and the chair for the work they have achieved so far. However, if a convention such as this is to have the desired effect I suggest that we need to consider not only how we ensure co-operation in order to obtain evidence, or intelligence, relating to criminal activities involving ICT, but that we also need to consider how we can ensure that such evidence is inherently trustworthy and can be used as effectively and rapidly as possible.

Without such a mechanism, capable of verifying independently that any data or evidence being supplied is reliable and trustworthy, we run the risk of creating a new mechanism which can be exploited by bad actors to spread misinformation about cybercrimes and subvert the overarching goal of frustrating criminal use of ICT - i.e. misinformation can be produced in a manner which makes it indistinguishable from truth - "false news", if you will.

Some progress on this has been made by the adoption of common quality assurance standards with the intention of allowing issues of admissibility to be resolved quickly through the provision of confirmation that minimum standards of scientific rigour and application of method have been achieved, thus reducing the need for potentially lengthy debate about evidence obtained in other jurisdictions using unfamiliar processes.

In light of this, may I humbly suggest that the that the Convention should include some reference to the adoption of, or work towards agreement on, the use of appropriate transparency, and/or quality standards, for evidence handling so that data/intelligence/evidence supplied by one party may be used safely by any other who requires to act upon it.

Relevant to this may be consideration of the ISO 17020 and 17025 standards, as preferred by the EU and International Laboratory Accreditation Cooperation (ILAC), or the ISO/IEC 27037, 27041, 27042, and 27043 group which are designed to be compatible with these standards, but more easily applied to the digital realm.

As I mentioned in my previous comments, the AHC may also wish to consider making recommendations about the adoption of a draft Convention on Electronic Evidence which has been prepared by a group of experts and which can be found at

- <https://journals.sas.ac.uk/deeslr/article/download/2321/2245/> or

- https://www.researchgate.net/publication/309878298_Draft_Convention_on_Electronic_Evidence

Such international agreement on transparency and verifiability is, I suggest, essential to allow rapid progress to be made towards countering crime as it is detected, and can achieve this by removing uncertainty about sources of evidence and the methods by which it has been produced. This is, I suggest, particularly relevant to the objective of "Developing measures, in particular establishing and strengthening competent authorities, to ensure the collection, obtaining and sharing electronic evidence."