Anglo American's presentation to the Second Intersessional Stakeholder Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

It is a pleasure to be with you all today, and to speak on behalf of ICC United Kingdom. I'm Craig McEwen, CISO of Anglo American. Anglo American is a diversified mining company with a global footprint across all major land masses. We are leading the way in mining, aiming to achieve carbon neutrality by 2040 with projects such as FutureSmart mining that will bring technology to bare in improving the efficiency and impact of our mining and NuGen, the worlds first Hydrogen powered heavy haul truck.

We are not a tech company – but cybersecurity, and effective measures to deal with cybercrime, are a major issue for us as a company. Like most organisations, we are moving towards a more digitised method of operating, connecting all parts of our business, and heavily relying on public cloud infrastructure to support our operations. Our size global presence and increased digitisation means we are impacted by opportunistic cybercrimes on a frequent basis. We also see specific targeting of our business, though this is less frequent than the later. Cybercrime impacts us not only in terms of lost revenue and productivity, but it impacts us on a more human level. It is often forgotten that cybercrime is just that; a crime and those who are impacted by it are victims. The impact on our colleagues, from embarrassment, to a more tangible feeling of guilt and other emotions that are often associated with traditional crimes take a toll on our colleagues. In an organisation where safety and wellbeing are central to our core values, this is something we wish to prevent at all costs.

The key to an effective outcome in our view is two-fold:

1. A focus on cyber-dependent crimes that are serious, have criminal intent, and are defined similarly across the vast majority of member-states. Right now, major multi-territory cybercrimes are costing industry billions a year, costing society even more, and growing at an alarming pace. Far too few perpetrators are facing justice. This convention will be a failure if it doesn't make a meaningful difference to that situation;
2. Effective measures to ensure cooperation between not only states, but also non-state actors and particularly the private sector, on an ongoing basis.

I'm going to focus on the second point here today.

For this convention to work, it requires ongoing, practical cooperation between authorities and the private sector. Aside from the convention, mutual legal assistance agreements will be needed to underpin the cooperation the convention calls for. Then, requests between jurisdictions will have to be evaluated by authorities and then passed on to companies. Companies will question the scope, clarity, or validity of some of those requests, forcing a two-way dialogue between national authorities.

This requires that officials both public and private know what to ask of each other, and where there is ambiguity or issues of conflict of laws, for them to work together to

resolve them - all in timeframes that do not allow criminals to continue to get away with their crimes, and for companies big and small, and countries at all levels of development.

Right now, this is often problematic. Many companies get requests that are too broad, too vague, or where providing the information asked for would violate the law in one of the concerned jurisdictions. That is the case even in developed countries with similar legal systems and long histories of cooperation on law enforcement.

This suggests to us that the Convention needs to anticipate these problems, and to create a process as part of the Convention itself where the parties, and stakeholders, can work together to identify common issues, and common responses. Where regional and international organisations like INTERPOL and EUROPOL and the bureaux and processes of other cybercrime-relevant instruments like the Budapest Convention can help and lend their expertise and experience.

At Anglo American we have directly experienced both the challenges, but the transformative impact collaboration can have. 24 months ago, Anglo American was targeted by a sophisticated group, known as FXMSP. We were approached by the UK's NCSC who provided details of darkweb communication relating to our business. This was not a formal process and relied more on a personally built relationship between myself and the NCSC. The information resulted in a length investigation, where information was shared between Anglo American and the NCSC. Eventually, the leaders of FXMSP were arrested and the USA issued an indictment against the group's leader.

Whilst we supported this investigation, the lack of formal process impacted timings, it is also likely that without that relationship, we would have been less likely to support, or even engage with the NCSC. Our sharing was done through an abundance of trust for a state instrument, however it was considered whether it was safe to share etc. before doing so. Concerns around law enforcement priorities impacting business decisions etc. were all factors that were taken at risk, in the absence of a formal agreement / norm.

We should not see this as an afterthought, but as something integral to the success of this Convention. We should seek advice from other similar processes now, to take the best those other processes have to offer us here. Perhaps it would take a parallel track to the negotiations to define what is needed on a multistakeholder basis and bring the result back to the formal negotiations.

What won't work is for states on their own to come to a political consensus around practical measures in treaty language without making an explicit effort to involve other sector stakeholders to review the text for fitness for purpose at a practical level. A political consensus around measures that won't work in real life isn't what the world needs.

I hope this has sparked both your interest and your imagination and I look forward to hearing what you have to say.