ICC United Kingdom	**Submission to the Fifth Substantive Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICT for Criminal Purposes**

ICC United Kingdom welcomes the opportunity to submit our views to the Fifth Substantive Session of the Ad Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

We deeply appreciate the ability of the private sector to participate in the work of the AHC. The modalities are an exemplar of good practice which many other processes in the international community could and should learn from.

We want to reinforce our strong support for the objective of a Convention that reduces the scope, scale, intensity, and impact of cybercrime globally. Industry is on the front lines of this fight and we have a material stake in a Convention that is fit for purpose. We also know from direct personal experience what works - and what does not work - in public/private sector cooperation on transboundary cybercrime. This Convention has a once in a generation opportunity to address the very real obstacles to effective cooperation; if it does it will have a significant positive impact on global cybercrime cooperation and we believe that opportunity must be seized.

In that spirit we provide comments below for the Fifth Session that build upon our previous submissions and interventions, particularly for the Third Session, here. We support the *Substantive Considerations on an International Instrument on Cybercrime* of the International Chamber of Commerce, and the statement of Microsoft made to this session.

Summary of Recommendations for the Fifth Session

1. **The Convention should focus on cybercrime and its prosecution rather than the use of information technology.** ICTs are tools used for many purposes; cybercrime is by definition socially and economically harmful. The convention should never lose focus on its purpose, which is to counter cybercrime and this is the term that should be used throughout;

2. **The Convention should address cyber dependent crimes serious enough to attract a minimum period of incarceration and not criminal acts which may be committed with or without the use of ICTs.** This has been addressed before but it bears reinforcing

given proposals in the current CND reference acts or processes which are not criminal, or that don't relate to criminal law. Moreover, there are references to offences which are already long-standing crimes that can be committed with or without the use of digital technologies. This Convention should stay focused on its essential purpose;

3. **The Convention must make clear that dual criminality is a prerequisite for all aspects of international cooperation.** This is essential because it is a prerequisite in practical application. The Convention should not contain provisions which don't fully reflect the objective reality of such fundamental elements of transboundary criminal justice cooperation;

4. **The scope of application of the chapter on International Cooperation should be limited to the offences described in the Convention.** This is doubly important as long as (i) there remain a long list of offences in the Criminalisation chapter that are not cyber-dependent, many of which are not widely recognised as criminal acts by most Member-States; and (ii) there are objections to basic provisions for safeguards;

5. **Principles of legality, proportionality, necessity, and transparency should be better reflected throughout the International Cooperation chapter.** There are many provisions which could be improved to better reflect these principles. Currently many States will refuse requests for access to data, especially data related to their own nationals, if they don't believe that the legal system of the requesting state has sufficiently robust provisions for human rights in a criminal law enforcement context. Ensuring that the Convention embodies the minimum protections that would allow all States to provide access to the data necessary for effective international cybercrime cooperation is therefore not just important, it is fundamental to whether this Convention will be successful.

6. **The use of terms should be consistent, and terms should be clear, specific, contextual, and relevant, especially in references to data access:**

    a. **The elements related to data protection need considerable revision** so that relevant terminology is used and the approach is congruent with best practices in data protection more generally.

    b. **Different terms should not be used to describe the same object or concept and terms should be specific and use the most appropriate term of art in context**. In particular, the term 'service provider' is too general, and is likely to result in requests sent to third parties who are unable to provide the information required. The term 'data custodian' is more specific and correctly identifies the third parties able to respond to requests related to this Convention.

7. **Reducing safe havens of cyber criminals.** The Convention presents an opportunity to reduce safe havens for cybercriminals irrespective of whether their activities take place in a State Party or not. This opportunity should be seized.

8. **Jurisdictional clarity and protection of victims:** One of the most important objectives of the Convention is to protect victims and, wherever possible, recompense them for the damage that crime has been done to them. We believe a few amendments would make this a reality. We

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

also urge negotiators to consider how expansive international cooperation provisions will intensify conflicts of law that may limit or prevent cooperation. In particular, negotiators should carefully consider the implications of a Convention that would encourage one state party to assert jurisdiction over a globally available online service provider to disclose data associated with a third country's nationals, merely because the provider's services were available to users in both countries. Instead, the Convention should encourage state parties to adopt laws - with robust human rights and due process protections - that establish jurisdiction over data custodians with legal presence in their jurisdiction but which recognize that international cooperation will be required to obtain data in many cases, including where the criminal acts, persons of interest, and/or data custodian(s) are located in another jurisdiction.

9. **Development and capacity building are fundamental to the success of the Convention.** As we have repeatedly highlighted, the Convention cannot be successful unless it ensures that all states who wish to become a party to it are able to implement all its provisions leveraging best practices on a voluntary *and* demand-driven basis.

10. **The Convention needs a mechanism for implementation that ensures all parties relevant to addressing cybercrime are a part of the process.** It is an objective reality that effective cybercrime investigation, prosecution, and redress for victims is impossible without public-private sector collaboration: the vast majority of the data necessary to cybercrime investigation and prosecution comes from the private sector. This argues for a step-change in the involvement of non-governmental stakeholders in the mechanism for implementation of this Convention compared to previous crime treaties.

Detailed Recommendations for Negotiators

Below are our recommendations in detail. We have also prepared a complete redline of the CND draft including the elements below, which we would be happy to provide to interested delegations.

The Convention should focus on cybercrime and not the use of technology or general cybersecurity concerns.

We believe that every provision of the Convention should be seen through the lens of its intended purpose, and part of that effort should ensure the text itself is focused. Therefore we recommend as follows:

1. Wherever the term ‘cybercrime’ appears in brackets it should be unbracketed and other adjacent options, such as ‘the use of information and communications technologies for criminal purposes’ should be deleted;

2. **The Convention should remain focused on the public sector, given it has exclusive responsibility for criminal law and enforcement.** Provisions on broader cybersecurity or other policy domains or which propose various forms of industry regulation should be removed; in many cases provisions would prejudge domestic choices about how to work with their own national stakeholders.

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

To address these issues, we recommend the following changes:

a. Delete Article 72(b), which could be read as allowing the officials of one State Party to directly address requests for cooperation to a data custodian in another State Party. This would impinge on the rights of the requested State Party, very likely create a conflict of laws situation for the data custodian, and erode trust and transparency.

b. Delete Article 76 (2). It should be replaced with a more general encouragement to pursue public private partnerships on a voluntary basis in pursuit of the objectives of the Convention.

c. Article 90 (2) has many elements that go far beyond cybercrime. However worthy some of the more general objectives are, most aren't within scope of this Convention. We recommend replacing this considerable list with a more general provision, perhaps paragraph 2 alone with the last sentence deleted.

The Convention should address cyber dependent crimes serious enough to attract a minimum period of incarceration and not offences which may be committed with or without the use of ICTs.

As we have noted previously, if this Convention fails to address major cybercrime incidents - which continue to grow in their number, extent, severity and visibility - it will be seen as a failure. We also know that existing international capacity for transboundary criminal cooperation is constrained even in major developed economies, and many UN member states do not yet have cybercrime legislation at all. This Convention should focus on these present realities and only address a broader range of offences later through its review mechanism if necessary.

Accordingly we recommend the following:

1. Preambular paragraph 3 should be amended to insert "particularly serious crimes" in the first line;
2. The word 'serious' should be inserted before 'crimes' in Articles 56 (2);
3. Add the term 'serious criminal offence/serious crime' to the terminology section of the Convention defined as "an offence that is punishable under the domestic law of both the requesting State Party and the requested State Party by a minimum deprivation of liberty of at least four years.";
4. Article 58 (1) should have the word "minimum" replace "maximum" - we believe this may be a typographic issue;
5. Article 57(1) should be modified to delete ", administrative or civil" - otherwise this Article could open the door to access requests for offences that are not criminal.
6. Paragraph 2 of Article 56 should be deleted as it extends application of the chapter to non-criminal offences;
7. Article 75 (1)(a) could be interpreted as extending the application of procedural and international cooperation to any crime that a State Party might "deem appropriate" so the following phrase should be removed: "including, if the States Parties concerned deem it appropriate, links with other criminal activities.";
8. Article 93 should be deleted; money laundering is already a crime and is not

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

cyber-dependent.

The Convention must make clear that dual criminality is a prerequisite for international cooperation.

1. Article 56 (1) should be amended to insert the principle of dual criminality alongside that of reciprocity in line 3, so that it would read "...principles of reciprocity and dual criminality…"

   This helps to make clear that the principle of dual criminality is fundamental to cooperation in the Convention.

2. Article 56(3) should be modified to read as follows:

   "In matters of international cooperation, ~~whenever~~ dual criminality ~~is~~ shall be considered a necessary requirement, and ~~it~~ shall be deemed fulfilled ~~irrespective of whether the laws of the requested State Party place the offence within the same category of offence or denominate the offence by the same terminology as that of the requesting State Party, or~~ if the conduct underlying the offence ~~for which assistance is sought~~ is a serious criminal offence set forth in this Convention."

   We note that Articles 61 and 68(3) provide for the refusal of cooperation where dual criminality is not established, which argues that the Convention should be very clear in defining dual criminality itself.

3. The last sentence of Article 58(4) should be deleted. That provision would automatically judge the nature of offences which may not always be the case in practical application.

4. The last sentence of Article 68 (3) should be deleted. It would waive the requirement of dual criminality where preservation is requested. Given the costs and procedural obligations that relate to preservation requests, and given these requests are generally received by the private sector, we see real value in ensuring that preservation requests are made where dual criminality exists.

5. If Article 69 is amended and not deleted as we recommend below, amongst other fundamental changes, paragraph 2 should be amended to add a new (c) reproducing the provision in Article 68 (4) so that the two articles, on expedited disclosure of preserved traffic data and expedited preservation of stored data, respectively, so that the dual criminality provisions for both are equivalent.

The scope of application of the chapter on International Cooperation should be limited to the offences described in the Convention.

Wherever the bracketed phrase "offences set forth in this Convention" appears, remove the brackets, and delete adjacent phrases with a different meaning. This affects, *inter alia*, Articles 56 (1) and 61(1).

Principles of legality, proportionality, necessity, and transparency should be better reflected throughout the International Cooperation chapter.

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

Ensuring these principles are embedded throughout the Convention is not just congruent with other international obligations and good practice, it will considerably facilitate the sharing of information transboundary investigations and prosecutions rely on. This is especially true for a convention intended to be applicable to all UN member states, where the instrument must create bridges across wide differences in legal systems, socioeconomic realities, and widely diverging levels of development generally. Companies, especially those that operate globally, have found that requests which take account of the proposals that we make below are far more likely to be successful, and more quickly, than those which do not. They also help ensure that the Convention will be congruent with member-states' existing international human rights obligations.

1. Article 58 (15) should be moved and precede current Article 56(4) modified as follows:

   "Nothing in this Convention shall be interpreted as imposing an obligation to ~~extradite~~ cooperate if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin, membership of a particular social group, or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons, or if there are substantial grounds for believing that the person would be in danger of being subjected to politically motivated persecution, torture, or inhuman and degrading treatment or punishment."

   These amendments restore this provision, drawn from UNCAC Article 44(15) which itself was drawn from Article 30 of the Refugee Convention, to the original wording from the Refugee Convention modified *mutatis mutandis*. The essence of the provision is excellent but should apply to the entire Convention and not only to extradition.

2. References to real-time collection of content data and traffic data should be deleted, given there will clearly not be a consensus to include them based upon the negotiations of the Fourth Session. This includes deletion of Articles 73 and 74, as well as other references.

3. Article 69 either needs to be rewritten or deleted. It has three fundamental problems:

   a. It addresses both real-time and stored content data without differentiating between the two despite the fact that very different legal rules apply;

   b. It suggests that one State Party can disclose to another data relating to the territory of a third State Party without the knowledge or authorisation of the third State party which creates multiple fundamental legal issues,, and;

   c. It unreasonably limits the circumstances under which the notified State Party may refuse to cooperate.

4. Any requests for assistance under the Convention must be made to all States Parties where there is any connection with the request; failure to do so risks conflict with fundamental principles of international law.[1] For these reasons, Article 72 (b) must be deleted as otherwise it allows for data custodians to be compelled to provide data held in a third State Party

[1] In particular the sovereign equality of states enshrined in Article 2(1) of the Charter of the United Nations.

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

without that State Party's knowledge or consent, an act which may also require it to break the law in one State Party to fulfill the request of another.

5. Add references to existing "international human rights obligations" *mutatis mutandis* in articles which currently defer exclusively to domestic laws, including Article 58 (14), Article 61 (3) and (4)(f), Article 74, Article 78 (1) and (2), Article 89 (10), and Article 94 (1) and (2).

6. Deletion of Article 78 (1) and (4). These provisions lend themselves to surveillance of persons generally in the first instance and controlling content online in general in the second. Neither are necessary for addressing cybercrime (and indeed as worded go far beyond criminal matters). The phrase "other persons concerned" is particularly problematic as this is disproportionate and could relate to persons with no connection to criminal acts at all.

7. Article 68 (7) currently has no time limitations on its operation. In practical application it is generally accepted that initial preservation is for a period of 60 days, with extensions allowed for a limited time, which must either be followed by a production order (with the data preserved until that order is received) or, if no production order is presented, the preserved data should be deleted. This suggests amendment of 68(7) to provide for the Requested State to notify the data custodian that a production order has not been received and therefore to delete the preserved data.

8. Deletion of the word "encrypted" in relation to platforms in Article 75 (1) (e) as this unnecessarily limits the scope of the provision to only encrypted illicit platforms; it could also be used to argue for undermining encryption which would be damaging to trust and security online more generally.

9. We would like to highlight the importance of Article 92(2). This covers, amongst others, penetration testers and security researchers (often known as "white hats"), when they do their work without authorisation but with the intent to help service providers of all kinds learn of security defects so they may be remediated before criminals take advantage of them. As we have repeatedly asserted, the Convention should proactively protect such activities from being criminalized. The criminalization chapter should address this deficiency but this provision should be retained as well.

Provisions should be improved in respect of transparency, to reflect that individuals have a right to know how, when, and for what purpose their data is used by governments, subject to ensuring criminal investigations and prosecutions can take place. data custodians should be able to disclose to persons (whether legal or natural) that their data has been disclosed to third parties - and in fact many jurisdictions require them to do so. Disclosure, and not secrecy, should be the rule as otherwise end users are unable to challenge decisions that impact them. It is also the case that in many countries, considerations about when and how to provide requesting states with information they request take into account how the requesting state will treat that data, so all states have an interest in increasing transparency and restricting the use of data to the purposes it was originally requested for.

Modifications in favour of transparency should be made, *inter alia*, to the following articles:

1. 61(17): to provide for notification of the data custodian by default;

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

2. 61(18): to require an explanation by the requesting State as to why confidentiality is necessary;
3. 68(2)(g): revise to provide that the requesting state must explain the need for secrecy and limit its requests according to Article 45(d);
4. 71(5)(f): add a clause to explain the need for secrecy in respect of these requests as well as the others;
5. 61(18), and 68(5), and 69 (2): provide that mutual legal assistance may be refused where the requested state believes that a human rights violation is likely to occur if the request were to be granted;
6. 71(6): require that the requesting state must follow up an oral request in an emergency with a written request expeditiously. Currently that is optional;
7. Article 58(9): require sufficient evidentiary basis for extradition; the current text is much more vague;
8. 58(4): Provide explicitly that extradition will not be granted for political offences;
9. 61(28)(b): making explicit that only records directly relevant to an investigation will be provided and that scope and nature of the request must be congruent with the principles of proportionality, necessity and legality;
10. Article 92(1)(d)(ii): This provision could be interpreted to restrict access to information on cybercrime on very broad grounds. We recommend deletion; it doesn't really add essential elements to the Convention.

The use of terms should be consistent, and those used should be clear, specific, and contextually relevant especially in relation to data access.

1. In order to take account of the previously-identified issues with how data protection is dealt with the term "data custodian" should be added in the terms section of the Convention, defined as "a person or organization who controls the collection, holding, processing or access to personal information which is the object of a request for cooperation under this Convention"

2. Except where the term "service provider" relates to traffic data, all such references should be changed to "data custodian."

3. References to specific classes of person in a crime context, such as witnesses, victims, accused persons, and persons of interest, should all be carefully reviewed to ensure they are consistently used; currently, the CND uses these terms interchangeably.

4. Terms such as "proper" (in the Preamble) which are subjective should be avoided in favour of objectively quantifiable descriptors.

Addressing the data of natural persons using best practice in international data protection

The provisions of the Convention related to data protection and access to protected data need revision to bring them in line with international best practice and simply reproducing the provisions of existing crime instruments without revision to take account of developments since they were drafted would not necessarily result in provisions that match modern reality.

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

Whenever possible, digital evidence should be sought from the entity that is closest to the person whose data is sought, for the simple reason that the entity with a direct relationship will have access to the data, whereas others will not. An example of this is a cloud service: many entities subscribe to cloud services as both public and private entities move their digital information to the cloud and use cloud-based infrastructure to deliver applications and services. However, that service only has access to the information of its customer, not of that customer's customers - and it is usually the latter information that governments seek access to.

With this in mind, whilst we welcome the general thrust of Article 57 we urge delegates to adopt further changes:

1. Remove the phrase "administrative or civil" in paragraph 1 as previously noted, to ensure a focus on criminal acts of a serious nature;
2. Amend paragraph 2 as follows:
    a. To make clear the requesting state is requesting, in both scenarios, data which the requested state is entitled to refuse. Currently the text does not provide for refusal;
    b. Ensure that any extension must be made in advance of the expiry of the initial period.
3. Amend paragraph 3 to ensure that data requested may only be used for purposes specified in paragraph 1.
4. Amend paragraph 4 to ensure records are kept of the manner and date of destruction of held data.
5. As previously mentioned in the transparency section, add a new paragraph at the end of Article 57, as follows: "The data custodian may notify persons when a State Party requests the disclosure of their personal [information/data], including traffic data, provided that doing so is not contrary to applicable law, and may publish the number of requests they receive from each State Party on a periodic basis."
6. A further new paragraph should also be added as follows: "This article is without prejudice to States Parties' domestic legal framework where it imposes conditions on the transfer of personal data to other States." This is needed to ensure that national law on data protection is not overridden by the Convention.

Finally, the Convention should seek congruence with the first intergovernmental agreement of common approaches to safeguarding privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes, adopted by the Organization for Economic Development (OECD) on 14 December 2022.[2] We recommend all delegates refer to the text as the AHC continues its work.

Reducing safe havens of cyber criminals

The Convention presents an opportunity to reduce safe havens for cybercriminals irrespective of whether their activities take place in a State Party or not. It can usefully do this with additional provisions, such as the following:

1. Amend Article 58(20) to include an obligation for States Parties to take appropriate measures

[2] The OECD Declaration on Government Access to Personal Data Held by Private Sector Entities addresses several issues which the Convention will address.

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

against states who intentionally harbour cybercriminals within their jurisdiction;

2. Amend Articles 61(19)(b) and 68(5)(b) by deleting the reference to "other essential interests" as valid to refuse mutual legal assistance. This is very broad and could be used to justify refusal to extradite criminals who would otherwise be extradited via the regular operation of the Convention.

Jurisdictional clarity and protection of victims

1. Returning proceeds of crime to its victims: Given that one of the most important objectives of the Convention is to protect victims and, wherever possible, recompense them for the damage that crime has done to them, we propose that Option 1 of Article 84 should be retained, and the others discarded. This option is the only one that requires for the proceeds of crime to be returned to the victims; other options make that optional and dependent upon national law.

2. The Convention should be clear on jurisdictional issues especially with respect to measures to identify, trace and seize the proceeds of crime in the interests of victims. Whilst Article 82(2) does this admirably, other articles, such as Article 40 addressed in the Fourth Session of the AHC, does not and should be modified accordingly.

Development and capacity building are fundamental to the success of the Convention

As we have repeatedly highlighted, the Convention cannot be successful unless all its States Parties are able to implement all its provisions leveraging best practices on a voluntary and demand-driven basis.

Additionally, we know that all states, irrespective of their level of development, have capacity constraints in their efforts to engage with other states on criminal cooperation to one extent or another. Ensuring more states are able to cooperate more quickly and effectively ought to be a shared goal.

Last, but certainly not least: stakeholders are indispensable in technical assistance and capacity building both as recipients and as implementers: as we have noted elsewhere, the vast majority of the data that is necessary for cybercrime to be dealt with is in private, not government, hands.

With this in mind, we recommend the following amendments to Article 87:

1. Insert references to voluntary collaboration with stakeholders, *mutatis mutandis*, in paragraphs 2, 3, 4, and 9;

2. Given that we know that conflicts of laws routinely arise, ensuring that States Parties and stakeholders are better aware of them and how to address them will help everyone. Therefore we propose to add two additional paragraphs at the bottom of the list in paragraph 2:

   "(p) Methods for addressing, and training to address, conflicts of laws arising where requests made by one State Party to another would require a third party to infringe the law in one State Party to cooperate with another;

   (q) Methods for addressing, and training to address, common issues in the formulation of

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk

requests for cooperation between States Parties that are refused."

Relatedly, we recommend the following amendments to Article 88 as well:

1. Insert references to voluntary collaboration with stakeholders, *mutatis mutandis*, in paragraphs 1 and 2 as well as 3(d);

The Convention needs a mechanism for implementation that ensures all parties integral to fighting cybercrime are a part of the process. It is an objective reality that effective cybercrime investigation, prosecution, and redress for victims is impossible without public-private sector collaboration: as previously mentioned the vast majority of the data necessary to cybercrime investigation and prosecution comes from the private sector. This argues for a step-change in the involvement of non-governmental stakeholders in the mechanism for implementation of this Convention compared to previous international instruments related to criminal matters.

Therefore we support Article 94, Option 2, with the following amendments:

1. Adding references to stakeholder contributions in sections (c) and (d) of paragraph 4;

2. Improve the value of input from stakeholders by amending paragraph 6 so that it makes clear unambiguously that submissions from stakeholders will be considered.

Finally, we don't believe that Article 94*quater* or 94*quinquies* should be retained. The Constitution of the ITU does not allow that agency to be involved in criminal justice matters; that is UNODC's mandate.

We thank the Committee for its consideration and look forward to further discussion of these issues during the session. We are represented at the Fifth Session in person; please feel free to contact our head of delegation, Mr. Nick Ashton-Hart, at nashtonhart@iccwbo.uk or +1 347 258 1676.

Headquarters: First Floor, 1-3 Staple Inn, London WC1V 7QH, United Kingdom
UN Office: % USCIB, 1212 Avenue of the Americas, New York 10019, USA
cyber@iccwbo.uk www.iccwbo.uk