Outcome Report of the Informal Multistakeholder Consultation on OEWG Zero Draft Report

The objective of the “Informal Multi-stakeholder Consultation on the OEWG’s Zero-Draft Report” was to collect the perspectives of non-governmental stakeholders on the zero-draft of the UN Open-Ended Working Group (OEWG) on developments in the field of information and communication technology (ICT) in the context of international security, so as to inform ongoing discussions of the OEWG. The event was held on 25 February 2021, ahead of the third and final substantive session of the OEWG. At the time of publication, the “first draft” of the report was released.

However, it should be noted that the discussions which took place and informed this report were conducted in reference to and on the basis of the “zero-draft”, and therefore all references to specific paragraphs of the report, should be understood to refer to the zero-draft.

The event began with opening remarks, and was followed by thirty-minute segments dedicated to each of the six substantive elements of the OEWG’s report: existing and emerging threats; rules, norms and principles; international law; capacity building; regular institutional dialogue; confidence building measures. Each segment was moderated by different experts (noted below). The report ended with closing remarks that summarised key themes and recommendations, also captured below. The recording of the event is available on www.letstalkcyber.org.

At each segment, participants were asked to focus their remarks on three guiding questions: 1) what is positive in the report/should be maintained 2) what should be strengthened or improved in the report and 3) what should be removed.

The four-hour event attracted some 200 participants from across the globe who actively participated in the discussions.

SESSION 1: EXISTING AND EMERGING THREATS

Time: *8:15-8:45 am*
Facilitator/co-facilitators: *Serge Droz (FIRST)*

SESSION OUTLINE

The session began with kick-off remarks from Serge Droz, Chair of FIRST, and was followed by a facilitated discussion. Participants were asked to focus on the three questions set out at the beginning of the event, focusing their remarks on the zero-draft of the OEWG report. Around 10 participants made comments verbally by taking the floor, while around five to six participants actively engaged via the chat function to offer substantive feedback.

ANY MAJOR THEMES / AREAS OF CONVERGENCE

What participants said they thought:

- *Was positive/good in the report*

There was general support for the report's suggested focus on a technology neutral approach, or on the use/abuse of technologies as the source of threats (as noted in paragraph 17 of the report).

- *Is missing/could be strengthened*
    - Many participants thought that the report did not put enough emphasis on the impact of threats and cyberattacks, suggesting further emphasis could be placed on vulnerable populations, and the impact of attacks on critical infrastructure, including for example healthcare facilities. It was suggested that infrastructure essential to public services should be considered critical infrastructure.
    - In addition, a number of participants pointed to the need to focus on evidence on threats to the basic ICT infrastructure, including for example threats to the supply chain (such as through remote access trojans or backdoors) and the public core. Increased emphasis on the responsibilities of both state and non-state actors to ensure that the ICT supply chain is secure is needed.
        - Two participants noted that the public core of the internet is synonymous with basic ICT infrastructure and that commitment has been made to protecting it. However, wider commitment to protecting the public core would support measures or actions that lead to reduced threats on the internet's core infrastructure
        - Another participant explained that a new Internet Governance Forum (IGF) coalition is working on this topic from the angle of making ICT products and services more secure and safer through government procurement and supply chain management and creating a demand for cyber security. This coalition is

seeking input from diverse stakeholders and encouraged reaching out to them.

    - A participant in the chat suggested that the report could be bolder in its references to state-led actions, including by calling in stronger terms for restraint and for ceasing state-led actions that perpetuate and escalate threats
    - It was also suggested that there be reference made to what is happening elsewhere in other forums, e.g a report on cyber mercenaries being developed in the UN Human Rights Council, and cyber-related vulnerabilities of existing weapons and weapon systems (nuclear, UAVs, LAWs, and online illicit trafficking of arms and dual-use materials of concern) elsewhere in the UN First Committee
    - It was suggested that the human-centric approach also be referred to in this section including that the human centric approach means recognising that vulnerabilities can have an impact on people and communities. Greater consideration of increasing reliance on digital technology in the future, including via increasingly connected systems (or IoT), an increased attack surface and the need for security by design in products and the development of internet standards was also recommended.

- *Should be removed*

Participants did not provide views on aspects of the report that should be removed, instead focusing (as noted above) on the aspects that should be included and/or strengthened.

RECOMMENDATIONS

- The report should put greater emphasis placed on the human and societal impact of malicious cyber operations, emphasising that it is humans who are impacted by cyberthreats and attacks
- The report should maintain the focus on the abuse of ICTs, and the behaviour of both state and non-state actors, not the technology itself
- In line with this point above, the report should put greater emphasis on the increased threats to critical infrastructure and to parts of the ICT infrastructure, including for example the public core and ICT supply chains, that require protection.

SESSION 2: Rules, norms and principles

Time: *8:45 – 9:15 EST*
Co-facilitators: *Nemanja Malisevic, Microsoft; Moliehi Makumane, DIRCO Republic of South Africa*

SESSION OUTLINE

During the session, all participants agreed on the validity and authority of the UNGGE 11 agreed norms. Participants also shared the zero draft assessment that the voluntary and non-binding, norms can help prevent cyber conflict and support socio-economic development. Norms complement and are consistent with international law, the principles of international humanitarian law and the promotion of human rights.

The implementation of norms requires a multistakeholder approach and continuous engagement. Threats in cyberspace cannot be tackled by States or industry independently, but all actors should work together to preserve and maintain peace and stability in cyberspace. Initiatives such as the Paris Call for Trust and Security in Cyberspace and the Oxford Process on International Law Protections in Cyberspace are two examples in that direction.There was agreement on encouraging States to initiate and support their multistakeholder approach at a national and regional level.

For many countries (primarily middle and low-income countries), the priority is understanding the implementation of the norms. In that respect, the Canadian Norms guidance was mentioned as very useful to support their implementation. Similarly, the Australian and Mexican Model Survey proposed to track implementation was mentioned as a good practice for all States to achieve consistency in reporting. However, while exchanging best or good practices on norms implementation is essential, it is crucial to recognise that no one size fits all.

The participants agreed that the process of understanding norms should be parallel to implementing the norms and developing new ones. Norms should be developed over time, and to respond to urgent concerns, they should include protecting the public core of the internet and healthcare facilities. Besides being consistent with International Law and human rights, new norms should not add additional burdens to Member States, and they should address legitimate gaps. They should be technology-neutral and non-discriminatory and should not place undue restrictions. New norms development should be done through multistakeholder consultations.

Reference was made to specific norms and States' responsibility to notify citizens and vendors of ICT vulnerabilities and adopt policies for responsible vulnerability disclosure.

ANY MAJOR THEMES / AREAS OF CONVERGENCE

What participants said they thought:

Was positive/good in the report

- Consistency of norms with International Law and human rights, and with a human centric approach to cyber security.
- The importance of efforts to operationalise norms
- The norms guidance described in paragraph 51 is a solid step in the right direction with regards to norms implementation.
- References to “parallel development of new norms” (paragraph 48) was welcomed, as is the conclusion that new norms could be developed over time (paragraph 57).
- Support was also provided for paragraph 55 on the protection of health facilities, recognised as an important step to the protection of health infrastructure.

Is missing/could be strengthened

- The possibility of undertaking a survey on norms implementation could be better included, to provide practical application of norms by states and disclosure of their views.
- Reference to relevant organisations in the Recommendations is not clear, and reference to only one stakeholder (i.e. UN) is not enough.
- The norm on improving security of ICTs, including supply chain security for ICT products and services should be explicitly spelled out in the Zero Draft, and encourage cooperation among states and other stakeholders on security of digital products and the supply chain.

- The report does not mention the need to engage and cooperate with all stakeholders in norm implementation (paragraph 49). It should explicitly recognise the role of non-state actors in norm implementation.
- The report should make reference to engage with other relevant initiatives, including other multistakeholder initiatives on cyber norms.
- Norms recommendations would benefit from clear guidance and monitoring mechanisms.
- Recognise that norms are not just consistent with international law but can also help states to interpret, apply and implement their international obligations.

RECOMMENDATIONS

- Place more emphasis on a multistakeholder approach to norms implementation, which should be a fully inclusive process. At the same time, highlight that there is a need also for disclosure of implementation and to monitor implementation of norms.
- Provide practical examples on multistakeholder cooperation, on how stakeholders are working on implementation of norms, or developing best practices on implementation of norms.
- Indicate that States, in consultation with other stakeholders should identify the relevant frameworks, such as national cybersecurity strategies and policies, where the norms can be operationalised at the national and regional levels.
- Encourage States to publish their position on how they interpret and how they want to operationalise norms. That would support monitoring and implementation.
- Actively encourage activities that help with norm dissemination.
- Annex the norms guidance described in paragraph 51 to the final report of the OEWG, to help diffuse the guidance contained therein, if it cannot be incorporated directly within the report.

SESSION 3: International Cyber Capacity Building Agenda

***Time**: 9:30 – 10:00 EST*
***Co-facilitators**: Annalaura Gallo (Cybersecurity Tech Accord); Chris Painter (Global Forum on Cyber Expertise)*

SESSION OUTLINE

Participants recognised the importance of Cyber Capacity Building (CCB) at all levels and that CCB is foundational to anything we do in the space of disarmament and responsible state behaviour in cyberspace. If states need to adhere to norms, they need the capacity to do so. There was also a general agreement on the importance to link CCB and development goals.

Discussants stressed that the CCB agenda should be multistakeholder and that it should be the multistakeholder community's responsibility. It was emphasised that the discussion on CCB should involve all stakeholders and that they have to be active participants in CCB activities.

The Zero-Draft was recognised as an improvement from the non-draft. Participants recognised that it is encouraging to see the importance of sharing best practices, as those are crucial to promoting cooperation among CCB actors. CCB efforts that emerge from the OEWG should build on existing efforts to avoid duplication and allow for synergies.

Cyber leadership is often an overlooked element. However, CCB should be holistic and most often, raising awareness among the highest office and decision-makers is of primary importance. International cooperation in this area is vital. At the same time, it was also stressed the importance of regional approaches to CCB and the critical role that regional bodies can play in this field.

A call was made for the need for more significant resources for CCB efforts. Participants supported an immediate increase in investment in CCB globally, especially in times of crisis when vulnerabilities might be amplified. Support can be provided in-kind, in the form of technical assistance or through other resources.

Important work in this area is already underway. Still, there is a need to reflect on efforts made and to leverage existing forums, for instance, the Global Forum on Cyber Expertise (GFCE) as a platform to foster global coordination, also considering that the principles on CCB in the Zero-Draft are those that the GFCE has put forward.

ANY MAJOR THEMES / AREAS OF CONVERGENCE

What participants said they thought:

Was positive/good in the report

- Principles to guide CCB efforts. In particular, participants welcomed the credit given to non-State stakeholders in capacity building and the principles stating that CCB efforts should respect human rights and be non-discriminatory.
- The recognition of the gender approach in CCB as critical.
- Para. 87, which recalls the value of South-South, South-North, triangular, and regionally focused cooperation is positive. It complements calls for more significant inter-regional exchanges in capacity-building, especially where priorities align more closely and naturally among developing economies.

Is missing/could be strengthened

- While it is crucial that women are being included in the OEWG process and that CCB should be gender-sensitive, the gender approach goes beyond this. For instance, regarding "the gender digital divide", it was suggested to include language to clarify that this divide must be addressed not only in human terms but also in ensuring that AI algorithms do not carry forward the gender (and other) biases of those who create them.
- There was support for the fact that the proposed survey to support norms implementation should also include CCB needs.
- Paragraph 88 highlights the importance of critical infrastructure protection for nation states' security and recognises the cross-border character of information infrastructure security.

However, the report should also specify the cross-border nature of critical infrastructures other than critical information infrastructures.

- Coordination among existing efforts should be placed in the prioritisation section, including reference to a vision for CCB. The UN should highlight existing multi-stakeholder efforts such as the Global Forum on Cyber Expertise in harnessing/consolidating existing CCB mechanisms to strengthen coordination, facilitate knowledge sharing, and connect requests for capacity-building support with resources.
- In Paragraph 82, the Capacity building agenda should be agile enough to adhere to the actual threat landscape, content and target group.
- Importance to stress that CCB has to evolve with time. States are at very different levels of capacity, and it is essential to address all stages.
- Considering that CCB might also occur in cooperation with CSIRTs across the globe, the report should include that CSIRTs should keep their neutral status and cooperate more with each other.
- A point not clear in the zero draft report is on the UN setting a global CCB agenda (Par. 82 positions UN as the lead for coordination on CCB). Importance should rather be placed on working together in a multistakeholder way. What is needed is instead harnessing - in a coordinated and well-funded way - existing mechanisms, forums and institutions that are already working on cyber capacity. This point could probably be added to Conclusions, par. 86 and principles within, along the lines of 'not duplicating the efforts but coordinating and harnessing existing CCB mechanisms, with the UN's role to ensure strategic political and financial support to these endeavours'.

RECOMMENDATIONS

- Paragraph 83 should be part of the conclusions and recommendations.
- Gender should be mainstreamed in the design, implementation and evaluation of capacity building programs.
- Reference to engaging non-state actors should be included in the recommendation section.
- The need for greater resources to be made available for CCB efforts should be included in the recommendations section.
- The CCB agenda should be survey-based and agile so that CCB is tailored to the countries' needs.
- CCB should be part of the wider sustainable development agenda.

SESSION 4: INTERNATIONAL LAW

Time: 10:00-10:30am
Facilitator/co-facilitators: *Dapo Akande (University of Oxford), Anne-Marie Buzatu (ICT4Peace)*

SESSION OUTLINE

This session began with kick-off remarks from Dapo Akande, University of Oxford and Anne-Marie Buzatu, ICT4PEACE. Diverse inputs were made from around ten non-governmental stakeholders and the International Committee of the Red Cross (ICRC) either verbally or by using the chat function. Many participants stressed themes of accountability; the need for better clarity as to how states interpret and apply international law; and international humanitarian law (IHL). There was also some acknowledgement and discussion about the interrelationship between capacity building, confidence-building measures, and international law; in that when states outline and explain the legal basis of their actions and measures in cyberspace, this builds confidence and capacity.

ANY MAJOR THEMES/AREAS OF CONVERGENCE

What participants said they thought:

- *Was positive/good in the report*
    - The reaffirmation of the general applicability of international law.
    - One participant urged that the references to IHL be retained, in particular:
        - The statement that "international humanitarian law has been developed and agreed by States with the objective to 'reduce the risks and potential harm to both civilians and civilian objects as well as combatants during armed conflict".
        - That report recalls that IHL "neither encourages militarization nor legitimizes resort to conflict in any domain." Other participants welcomed and urged retaining this (in paragraph 29).
    - Maintain the more specific references to the key principles of the UN Charter and from within international law, such as those found in paragraphs 28 and 34. There could be a corresponding conclusion or recommendation.
    - It was noted that there is no explicit mention of the existing duties of states to prevent malicious cyber operations.
    - The point was made that in paragraph 30, the zero draft says that states "should seek to ensure their territory is not used…". However, this overlooks that international law already provides for an array of obligations in this regard and so the language should be changed to "must".
    - One participant noted appreciation for paragraph 30 re-affirming the norm against use of proxies. It was also noted however that the current wording of this paragraph suggests that this exists as a policy recommendation rather than an existing principle of international law (which it is), or that the obligation only exists for actions of non-state actors that are attributable to states.

- *Is missing/could be strengthened*
    - The report could be strengthened if it was acknowledged that international law *in its entirety* applies; the current formulation of paragraph 27 somewhat implies that only the UN Charter applies in its entirety.
    - Diverse participants noted that there are no references to, or meaningful discussion about, about oversight or accountability.
        - One organization referred to its proposal for a peer review mechanism on State behaviour in cyberspace on the order of the Human Rights Council's Universal Periodic Review (UPR) mechanism.

    - There needs to be a way for states to clarify their views on how international law applies.
        - Suggestions were made to switch how paragraph 41 is worded; either to a formulation in which the UN Secretary-General would solicit views, or to use stronger language such as "States are *strongly encouraged to….*".
    - It was encouraged that states should go one step further and affirm by consensus that IHL principles of humanity, proportionality, and distinction, among others, impose well-established limits on cyber operations during armed conflict and do not encourage militarization of any domain, and are without prejudice to States' obligation to settle disputes peacefully and to the prohibition on the use of force.
        - § States were encouraged to discuss the subject of limitations to cyber operations during armed conflict in any future or sub-group of the OEWG.
    - One organization made reference to its proposal that states publicly commit to not attacking critical infrastructure. Such a call to action or commitment could be included in the report/recommended by the OEWG.
    - It was hoped that in light of on-going development of military cyber capabilities, states could agree on re-affirming certain IHL principles that protect civilians.
    - An explicit mention of the "no-harm rule" was suggested by one participant, which is a recognised principle of customary international law with respect to the environment. This is not included in the zero draft.
    - One participant noted inconsistencies between the sections of the zero draft on Threats, and on International Law. For example, paragraph 9 says that international security cuts across multiple domains and disciplines, which is correct; but then subsequently mentioning cyberspace as a domain is misleading because it gives the impression that this is an exclusive zone. This could be clarified.
    - One participant noted that the zero draft makes clear the interrelationship between ICTs, international security, and international war. It was suggested that the report could recommend establishing a research and monitoring centre.

- *Should be removed*
    - *n/a*

RECOMMENDATIONS

- The above section outlines specific recommendations from participants who spoke or contributed in writing during this session. Some are recommendations that would give precision and accuracy to the report, while others are calls for stronger language or in some cases, new conclusions or recommendations.
- A general recommendation shared by most participants is that states need to move beyond the general acknowledgement about the applicability of international law to their cyber behaviour and in using ICTs and really begin to describe and outline what this means practically, how they interpret the law, and on what legal basis relevant actions stand.

SESSION FIVE: Regular institutional dialogue

Time: *10:30-11:00am*
Facilitator/co-facilitators: *Ambassador Henri Verdier (France), Allison Pytlak (WILPF)*

SESSION OUTLINE

The session began with kick-off remarks from Ambassador Henri Verdier of France and Allison Pytlak of the Women's International League for Peace and Freedom (WILPF). Ms. Pytlak's kick-off remarks noted this topic had been a vibrant aspect of the discussion within the OEWG, leading to the proposal from France and other states to establish a cyber programme of action (PoA) on cyber, and also that a second OEWG has been established, amid controversy, by the UN General Assembly. While it's hard to determine common priorities from across all civil society on this point, Pytlak noted that in past statements and events, many non-governmental stakeholders have stressed themes of inclusivity, transparency, and meaningful participation. Amb. Verdier outlined in greater detail the proposal for a cyber PoA. He explained that as a politically binding instrument, a PoA is a good bridge between calls for a legally binding treaty and the existing normative framework. He emphasised that the PoA would offer the benefit of creating a permanent forum within the UN system for international cyber security; would help to foster accountability for all actors; and be based in pragmatic actions.

During the discussion, there were fewer direct reactions to this section of the zero draft than had been heard in other segments of the event and more discussion and exchange.

ANY MAJOR THEMES / AREAS OF CONVERGENCE

What participants said they thought:

- *Was positive/good in the report*
    - One organisation said it agreed that there is a need for more actionable, permanent discussions and so a Programme of Action, dependent on meaningful and inclusive mechanisms for civil society participation, could support the widely recognised need for existing commitments and recommendations, including developing guidance to support and monitor their implementation; coordinating and strengthening the effectiveness of capacity-building; and identifying and exchanging good practices. Another organisation also said it believes it is time to move to more action-oriented dialogue.

- *Is missing/could be strengthened*
    - One participant highlighted that there was no mention of the fact that a lot of cybersecurity incidents are the result of decades of focus into features and innovation that have sacrificed security in negligent ways. A "secure by default" framework framework was encouraged to minimise the problem, which can be easily adapted into each state's own law.

        - Somewhat related, another participant observed that the role of human decision-making within international cyber security is absent from the draft.
    - There is a wide range of learnings that can and should be leveraged from other forums, including the implementation of other Programmes of Action in order to ensure meaningful inclusivity in any future regular institutional dialogue.

- *Should be removed*
    - *N/a.*

RECOMMENDATIONS

Some participants made recommendations and observations during this segment that are broader than textual suggestions for the zero draft of the final report:

- There was discussion about the human element and role of individuals in cyber security decision-making, as well as about what basic standard or level of security should be expected. Even while these are technical discussions, the role of individuals within them should not be overlooked. One participant built on earlier discussion and comments about doing more to build in security at the outset of a product's development process but noted that there is little incentive to do so. This participant encouraged to "level the playing field" and asked everyone to engage in "secure by default" processes in order to allow everyone to innovate without sacrificing security. This approach could combine with building trust, confidence, capacity, and awareness to enable a new security cyber environment.

- Finally, and while not framed as a recommendation, there was some discussion in this segment about the new (second) OEWG that will begin work later in 2021, including the problematic way in which it was established and that the potential for non-governmental stakeholder participation is not yet determined.

Session 6: Confidence-building measures (CBMs)

Time: 11:15-11:45
Facilitator: Gregor Ramus (OSCE)

SESSION OUTLINE

The session opened with an introduction by Gregor Ramus from the Organization for Security and Co-operation in Europe (OSCE), who offered remarks on CBMs as discussed in the Zero Draft Report from the OSCE perspective.

OSCE is encouraged by the recognition in the Zero Draft of the efforts that regional and subregional organizations have made in developing and implementing CBMs. Regional organizations have contributed to both OEWG and GGE and would welcome exploring how the involvement of regional organizations in the UN level deliberations could be further formalised. OEWG provides an excellent opportunity to formalise such a kind of cooperation. The Zero Draft recognises the value of regular inter-organizational and interregional exchanges of lessons learnt and good practices. To take full advantage of this cooperation it would be welcome to further explore the possibilities of holding regular exchanges between regional organizations under the UN auspices. The Zero Draft further recognises the importance of creating networks of national Points of Contact (PoC). OSCE stands ready to cooperate closely with the UN structures and to share experiences and best practices. OSCE's CBM 8 Point of Contact network can serve as an example of the value of such networks. OSCE welcomes the discussion on establishing a global repository of CBMs under the UN auspices. As already indicated in the Zero Draft, it should be emphasised that CBMs should not only be implemented on the national and international level but also on the regional level with the support of regional organizations, where applicable.

What participants said they thought:

Was positive/good in the report

- There was a general agreement among the participants that the section on CBMs in the Zero Draft was well developed and captured their most important points.
- It was appreciated that the Zero Draft reinforced the importance of CBMs as well as recognised the importance of their effective and of information sharing and gathering best practices as the implementation of CBMs can strengthen the overall resilience and security of ICTs.
- The inclusion of national Computer Emergency Response Teams (CERTs) as essential to ensuring that CBMs serve their intended purpose was mentioned as a positive aspect being included in the Report.
- The report has recognised the role and added value of the Points of Contact (PoC) networks, which even though difficult to maintain, are essential elements that should be retained, whether regionally or on a global level.
- The report's mention of the desirability and viability of establishing a global repository of CBMs under the UN auspices was welcome as a positive step.

- ***Is missing/could be strengthened***

  - The OEWG report should go beyond general statements and include more actionable language when referencing that states should actively undertake developing global CBMs while taking into account what has been done on the regional level, and start to identify good practices.
  - The OEWG report should include a reference to the role of non-governmental stakeholders. It was suggested adding a reference to the role of non-State stakeholders in paragraph 73 of the CBMs section: "States voluntarily identify and consider CBMs appropriate to their specific contexts, and cooperate with other States, as well as non-State stakeholders, on their implementation."

- ***Should be removed***
  - n/a

RECOMMENDATIONS

- *Formalised regional exchange.* Regional organisations play an important role in translating CBMs into practice, including through information exchange, capacity building, and gathering of best practices. At the same time, dialogue between different regional organisations, as well as complementary dialogue at the global level, can support CBMs adoption. There is a further need for formalisation of the regional exchanges on a regular basis under the UN auspices to avoid leaving this exchange on an ad hoc basis.
- *The role of non-state actors.* In different national and regional initiatives, non-governmental stakeholders are actively involved in the discussions on how to implement CBMs. Non-governmental stakeholders can play key roles in capacity building, as well as in the design, implementation, monitoring and evaluation of CBMs. The report recognises that there is a variety of multi-stakeholder initiatives that exist to contribute to CBMs, but the text could be stronger on the need for greater transparency and information sharing on the implementation to assess their effectiveness in different contexts and this way contribute to more effective implementation. There is a role for other stakeholders including CSOs in supporting the understanding of their effectiveness and the report could include this reference in stronger terms and in the recommendations.
- *Actionable language.* The desirability and viability of establishing a global repository of CBMs under the UN auspices included in the report were welcome, yet a more actionable language referencing that states should undertake concrete steps toward developing global CBMs would support progress and move the discussion beyond more general statements.
- *Greater transparency.* States should be encouraged to take more measures to be transparent about their behaviour, whether by publishing policy documents on the cyber policy portal or otherwise. This would help to understand the motivations behind certain actions and developments and build among state and non-state actors.