Submission of the OneGoal Initiative for Governance to the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies – July 2022
by Alève Mine for the OneGoal Initiative for Governance, July 25, 2022

As an independent endeavor, the OneGoal Initiative for Governance (henceforth “the Initiative”) makes this submission to the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies (OEWG).

Introduction

The OneGoal Initiative is young and can be described as an effort to tackle risks, chiefly risk recursion, that are not covered elsewhere such as in the SDGs or through current governance processes.

The following issues with regard to cybersecurity and privacy are submitted for consideration.

Overarching remarks

Inter alia, issues of legal defense capacity, economy, cyber security, insurance and finance are by nature interlinked and interact even when linkages are not officially considered when focusing on one of these items. As a result, consequences of decisions regarding one item on other items across states will clarify the partiality of said decisions. In the case where these considerations will not be integrated into the main OEWG line of work, the launching of a thematic group would be in question.

In discussions it may further be useful to keep in mind that decisions made in the context of cybersecurity may impact on space law due to similarities, and to accordingly proceed with foresight.

Cybersecurity in relation to the economy

Cybersecurity breach event-related damage and costs, being typically overwhelming at any scale, firstly directly due to any resources obtained by successful violators, secondly due to the impact of disruption or damage, and thirdly due to lawsuits or fines in relation to cybersecurity operations, attention should be drawn to any non-insurability of those risks. Indeed, where a large and growing insurance market opportunity exists, ways to finance the unfinanceable will be creatively sought, potentially leading to partial (meaning not affecting all actors to the same degree, or in the same polarity or direction) economic damage larger than that encountered in the Great Recession through uncompensated risk- and cost transfers onto third parties such as governments, individuals, pension funds or private enterprise that doesn’t interfere with the insurer’s stakes when going bankrupt. This would be likely to trigger social unrest and leave
permanent scars on the impacted economies, potentially making them subsequently more dependent on third parties for their survival and development, and would happen in the absence of cyber violations. In addition, impacts can also include less obvious, more diffuse or more precisely targeted, diversified or gradual impacts that blend into the wider range of changes and crises occurring in economies and societies worldwide, possibly exerting a large compounded impact that remains undiscerned.

The damages in question can be larger than those of cyber violations themselves in the same time window.

The basic principle required to prevent these is: if an insurance is not financeable, this will not be attempted to be overcome through financial product structuring, tax exemption or haven, or enterprise risk management. Other categories of solutions must then be sought. Accordingly, when this principle is applied, care should be taken not to disadvantage the insurance industry relative to other industries from a policy point of view.

It is to be noted that, purely theoretically speaking, considering that cyberspace violators are not typically identified, cybersecurity insurance, capacity development-related investment or -lending, policy-making as well as cybersecurity services industries could create their own markets or fields of activity at will, until their market, or indeed their consumers or clients, are exhausted in every sense of the word. It is here proposed that such possibilities should not be left unconsidered.

Furthermore, the level of control of insurers over their clients with regard to measures client candidates are required to take in order to be eligible for insurance creates a substantial operational decision power and financial pressure of insurers over their clients.

As a general principle proposed here, the party that profits, be it from a reputation, strategic positioning, financial, operational or other perspective, from a process they launch for said advantage should also carry the risks that the process generates for third parties.

Objections to the consideration of this issue in the framework of the OEWG are possible because its solution lies in financial regulation. What this nevertheless means is that the regulation of financial products and of business entities such as captives should be coordinated with the regulation of cyberspace.

Cryptography vs foregoing encryption practice

A theme to be discussed is the so-called “quantum apocalypse”, for which the technology may be ready at different dates for different actors and remain inaccessible to other actors. This is relevant for the security of many professionals and witnesses, but also for all other persons and entities. A restriction to the use of quantum computing (or other future decryption capability, to be

---

1 This makes the categories of international and non-international armed conflict for the purpose of the application of IHL problematic.
thorough), restriction that would selectively, only under certain conditions and exclusively for certain uses, allow parties to decipher collected data, should be agreed upon. This may not only protect persons, but also prevent some parties from having an incentive to make the development of this technology inaccessible to some other parties. This may matter not the least because, once said technology is in use, communications using inferior encryption will be potentially unreliably, making users dependent on providers of quantum technology and the latter a large, and to some inaccessible, market.

Until said technology breaks current encryptions or said agreement exists, persons who may feel concerned, which could be individual, private, non-governmental including humanitarian, or governmental actors as well as special rapporteurs, can do little else than avoid communicating digitally (unless organisational solutions or mechanisms already exist to that end), which may reduce their capabilities to such an extent that it would not be a viable solution.

In that regard as well as for other purposes, it is proposed to add the responsibility of individual-, private-, civil society-, international- and supranational actors to the non-exhaustive selection, already proposed by colleagues, of international law topics to be prioritised in any future proposed program of work for the current OEWG.

The above supports the two points about confidentiality in paragraph 86 of the Zero Draft.

**Attribution of responsibility**

Due to the non-triviality of identifying violators of cyberspace, and due to the growingly multifaceted interdependencies between private and state actors, the precision of any attribution of responsibility, including a differentiation between state actors and private actors, suffers. On the one hand, attribution may let some responsibility remain unmet and some possibly erroneously attributed, and on the other hand, not identifying violators would require another strategy to discourage violations.

In the absence of a viable solution for the latter, a below-the-surface analysis of responsibilities, impacts, risk transfers and interdependencies, at, inter alia, economic, strategic, and other levels is required, along with the use of such information in legal action.

In this, responsibility can be a distributed matter, and, should the case be, should be considered as such in court.

Furthermore, a system can be funneled toward an outcome through small, under-the-radar actions that either simultaneously or sequentially, possibly in conjunction with other events, lead to a decisive impact. Therefore, a drivers- and outcomes-based approach is proposed for the here recommended analyses.

Ultimately, such analysis should be routinely executed and a database thereof established.
In addition, if one party is, for any reason, unable to proceed to such an analysis or launch an effective legal action as shown by such information to be relevant, a provision should be established by which these tasks, with fiduciary duty, will be fulfilled on that party’s behalf. Indeed, the ability to defend one’s rights has economic outcomes, and failing to provide for the above means that each state’s outlook is systemically eligible for damage in the same manner, depending on circumstances, and circumstances sometimes evolve, at any pace, in unforeseeable ways.

Further is encouraged the consideration of the following question: What in the character of a certain level of damage caused by a cyber violation perpetrated by a private actor makes it less qualified for an individual or collective self-defense than the same level of damage caused by a cyber violation perpetrated by a state actor?

**Technology and laws**

Technology, organisation, laws, social structures and geography are examples of attributes that shape the landscape on which each actor proceeds to unfold their norms, policies or strategies. In that sense, technology is not a neutral object and can, all other things being equal, favor one or the other process or activity. Therefore, while we may stay open to technologies, when structures such as laws and policies are built without taking into consideration the impact of a technology on the landscape, or topology, in which we function, the outcome will be modified depending on the technologies used.

Here is a transposed example for the mere purpose of conveying part of the ideas above: If there was an intruder in your house while you were there, chances are you would see the intruder, and if the intruder took pictures of any documents or of your interior, you probably can confiscate these if the police intervention goes well. Comparing this with cyberspace where an intrusion goes unnoticed and only copies some of your files, this would be as if the intruder in your house used an invisibility cloak and didn’t catch your eye. This would probably not make it legal for them to be in your house and make copies of your private documents.

Here is another such example: if someone entered a country to damage local assets, which they succeeded in, then flew away again, this would constitute a crime and the actor be searched for, and where possible reprimanded, through international collaboration. This transposes as a cyber violation onto a private individual or -enterprise. If this is not investigated with a similar effort, then remains to be defined the aspect of the act’s digitalness that makes it less of a crime. Other factors, such as a possible lack of resources for such an investigation, can exist, in which case the issue should be discussed directly and remediated accordingly.

As laws are sought to be applied to cyberspace, it is not the application of the law as is, but the application of its **original purpose** that would, when applied to the **new landscape**, have a chance of leading to the desired outcome.
This is nevertheless not an issue in the case where a text of law is formulated in a way that expresses its very purpose immediately (which means in a more abstract manner), or in the case where the portion of the topology touched by a text is disjunct from the portion of the topology that is modified by a given technology.

This may provide an anchor when considering paragraphs 34 and 37 of the Zero Draft.

**Consensus**

During a consensus-building effort, not least in a global security effort such as the one carried by the OEWG, particular care should be given to make sure that a consensus is not being reached by muting dissenting voices or letting them self-censor under the pressure of time, peers or delicate circumstances.

**Evolution of cyber**

The evolution of cyberweaponry vs cyberdefense is escalatory in character, potentially, if not already today, leading to an unmanageable state, requiring too large a part of our resources or a rise in other types of risks, especially in a world dealing with further substantial threats.

Furthermore, the time, effort, energy and other resources taken by cybersecurity-related activity are all taken out of the resources available to fulfill the respective functions of the insured and the breachable.

With these in mind, an additional track of discussion is suggested to be held over the long term, that identifies and where reasonable, in a positive sense, removes the reasons, respectively motivations, for any actors to desire to realise a cyber violation, because among the numerous parties partaking in violations in cyberspace, an ultimate deterrent doesn’t exist.

**Conceptual remark**

The object of the work of OEWG is only one aspect of the common system of which each party is, in turn, only a part. The optimization of each partition along those two dimensions as if each partition was a standalone system to the exclusion of the others would necessarily, in a sense mathematically, bring about a worse outcome for each party and object. Indeed, as compared to the unified optimization of the overall system, this would, for each partition, raise the floor of risks and damage starting from which a partition-centered optimization can be sought.

The prerequisite for this last affirmation to be correct is that the overall goal pursued matches the functional topology of the overall system, failing which any outcome and any decision brings about losses. That said, the optimization of the partition’s goal with the same approach necessarily leads to the adoption of an overall goal, therefore partition-centered goals are always sub-optimal.
Today more than ever, the future depends on the human ability and readiness to make decisions based on abstract thinking. Indeed, the more fundamental, high leverage issues humanity faces are not available for scrutiny at a concrete, pragmatic, past facts level.

Therefore, while the abstract quality of this remark may blur its relationship to the urgent concrete needs of the parties to the OEWG, it helps to consider that for instance physics formulas, albeit abstract, have rather unyielding impacts in practice, that constitute an immediate basis for action-oriented decisions.

It perspires that, in order to avoid losses on all sides:
- Care should be given in this week’s talks to make, no matter the current situation, a future unification of goals possible;
- The common goal to then be aimed for must, and this requires an elaboration that is outside of the scope of the present text, match the functional topology of the total human system;
- Deliberating some topics to the exclusion of or detached from others cannot lead to an optimal result, whereby when topics are discussed in the light of each other, this must be done in the framework of the above common goal.

Feedback and Comments

The OneGoal Initiative welcomes feedback, comments and expressions of interest for partnerships for its development and implementation, from all parties, via aleve@onegoalinitiative.org and other channels.