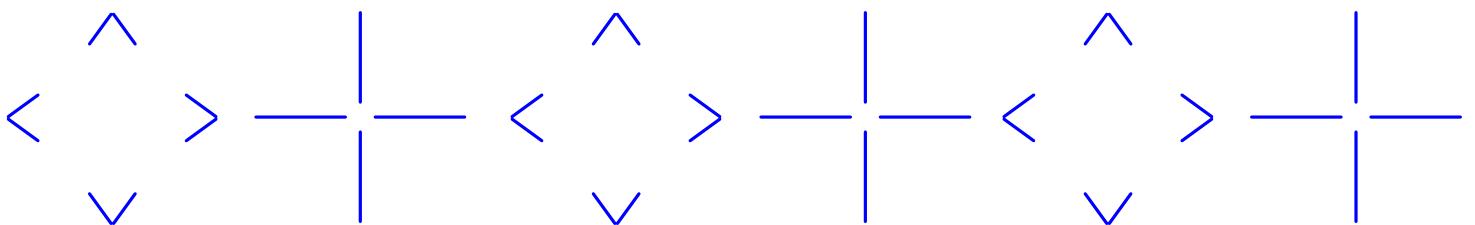
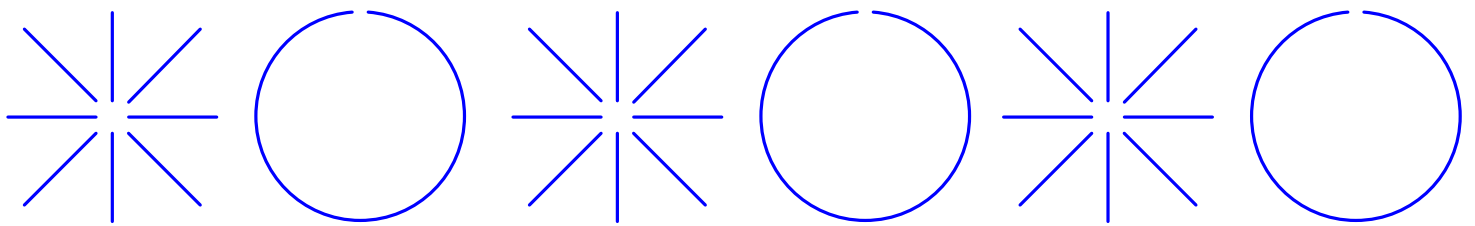
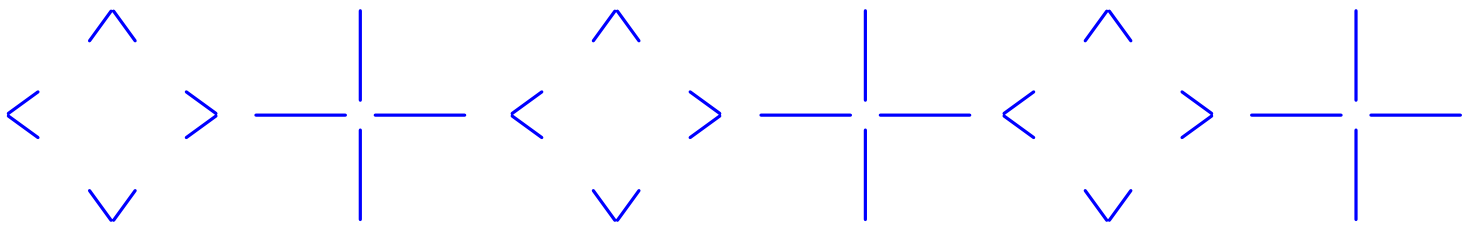
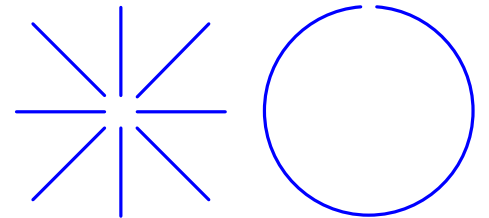




REPUBLIC OF ESTONIA
MINISTRY OF FOREIGN AFFAIRS

TALLINN WORKSHOPS ON INTERNATIONAL LAW AND CYBER OPERATIONS

Compendium of reports
2023



Contents

- 3** **Preface**

- 4** **I Tallinn Workshop on International Law and Cyber Operations, 21-22 February 2022**
 - 1.1 Opening remarks and introduction
 - 1.2 Peaceful settlement of disputes
 - 1.3 Sovereignty
 - 1.4 The principle of non-intervention

- 14** **II Tallinn Workshop on International Law and Cyber Operations, 6-7 June 2022**
 - 2.1 State Responsibility (legal focus)
 - 2.2 Attribution (strategic, policy focus)
 - 2.3 Retorsions

- 23** **III Tallinn Workshop on International Law and Cyber Operations, 3-4 October 2022**
 - 3.1 Use of force
 - 3.2 Countermeasures
 - 3.3 Self-Defence

- 31** **IV Tallinn Workshop on International Law and Cyber Operations, 30-31 March 2023**
 - 4.1 The notion of an “attack”
 - 4.2 Objects: dual use and data
 - 4.3 Categories of persons involved in hostilities during armed conflicts

Preface

Malicious cyber activities are on the rise and amplified by the increasingly complex geopolitical setting. In order to tackle these challenges, countries are working towards strengthening their resilience in cyberspace. Estonia has always underlined that the foundation of enhanced clarity, predictability and stability in cyberspace lies in the adherence to international rules-based order. With the aim to support the discourse on international law, the Estonian Ministry of Foreign Affairs, in cooperation with the Estonian Ministry of Defence and in coordination with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), initiated in 2022 an informal process called the Tallinn Workshops on International Law and Cyber Operations.

The main objective of these topic- and scenario-based workshops has been to create a forum for informal discussions between NATO CCDCOE members and partners as well as offer the opportunity to examine the most pertinent international law issues related to state conduct in cyberspace. Such discussions assist in establishing where both commonalities and diverging views may lie, thereby advancing the understanding of relevant concepts of international law. The workshops have also presented a possibility for exchanging views in the context of ongoing international processes and consultations.

Hereby I am glad to share with you the reports of the four Tallinn workshops held during 2022-2023. The topics covered included peaceful settlement of disputes, sovereignty, non-intervention (*I Tallinn Workshop on International Law and Cyber Operations, 21-22 February 2022*); state responsibility, retorsion (*II Tallinn Workshop on International Law and Cyber Operations, 6-7 June 2022*); use of force, countermeasures, self-defence (*III Tallinn Workshop on International Law and Cyber Operations, 3-4 October 2022*), and attack, dual use and data, categories of persons involved in hostilities (*IV Tallinn Workshop on International Law and Cyber Operations, 30-31 March 2023*).

I hope that this compendium not only conveys the intricate discussions held during the workshops but also contributes to building an understanding on how existing international law applies in cyberspace.



Minna-Liina Lind

Undersecretary for Global Affairs at the Ministry of Foreign Affairs of Estonia

A handwritten signature in blue ink, which appears to read 'Minna-Liina Lind'. The signature is fluid and cursive, written in a professional style.

I Tallinn Workshop on International Law and Cyber Operations, 21–22 February 2022

The following summarises the discussions held at the I Tallinn Workshop on International Law and Cyber Operations, held in Tallinn on 21–22 February 2022. The workshop featured, inter alia, presentations and discussions led by Ambassador Takeshi Akahori (former Japanese Ambassador for Cyber Policy, currently Ambassador for Global Affairs) as well as Dr Russell Buchan (Sheffield University), and was conducted under the Chatham House rule. The summary includes references to the scenario-based discussions held during the workshop.

1.1 Opening remarks and introduction

Before the discussion on peaceful settlement of disputes, the Tallinn Manual 3.0¹ process was introduced. A lot has happened since 2016 when the Tallinn Manual 2.0 was finalised. States are increasingly comfortable with publishing their national positions and there have been several examples of cyber operations in relation to the pandemic and elections. There are many issues being discussed by States such as *domaine réservé*, coercion, sovereignty, non-intervention. The new revised Tallinn Manual 3.0 will have a similar structure to the previous 1.0 and 2.0 editions. States will be approached to clarify the commentary. The end result will be academic work, not law. The Tallinn Manual 3.0 may include new rules in commentary as well as expand to new areas such as investment law, trade law, and environmental law issues. There have been significant discussions on collective countermeasures, due diligence, sovereignty (especially the threshold of its violation), and intervention (especially regarding the topic of required coercion). It was reminded that the Tallinn Manual process is looking for crystallization, whereas there is a difference between interpretation and actual customary international law. The planned timeline for the Tallinn Manual 3.0 process is as follows: reaching out and State engagement in 2024–2025, finalising the manuscript in 2026 and publishing in 2027.

1.2 Peaceful settlement of disputes

After the opening remarks, the workshop began by discussing issues related to the peaceful settlement of disputes (PSD). The discussion began with a comprehensive overview of how these issues are covered in UN GGE as well as OEWG processes, the Tallinn Manual 2.0 and the UN Charter. In particular, the presentation pointed out references to the PSD in different interpretations put forward by different nations (e.g. in the format of State positions as annexed to the UN GGE report). Finally, the presentation underlined several important cases of the International Court of Justice (ICJ) such as the Nicaragua and Corfu judgements in offering clues on how to substantiate the PSD obligation.

¹ More information at: <https://ccdcoe.org/research/tallinn-manual/>

Several participants underlined the value of discussing in greater detail the topic of PSD, which used to be more of an academic exercise before but has now also entered international debates. Others remained cautious and asked about the practical value of PSD in the current complex security environment. The following discussions held in open plenary as well as in the format of breakout groups underlined several open questions and topics in relation to PSD.

1. **Background discussions at the UNGGE and OEWG.** It was shared that while the UNGGE/OEWG reports mentioned PSD, the processes could not (yet) go into further detail regarding how to apply the obligation for PSD. However, there was consensus in the UNGGE discussions that there was a need to include the topic of PSD, and references to Article 33 of the UN Charter were made in discussions. There is hope that the OEWG process could go deeper in the interpretation of PSD. One of the aims in the UNGGE was to provide a larger number of tools to victim states. States were invited to implement the UNGGE and OEWG reports, and to quote international law, the GGE reports and national positions when attributing. It was also discussed whether the UNGGE/OEWG processes would be willing to go into more detail with the PSD obligation.
2. **What is a dispute, what is an international dispute (and does it even matter)?** One participant underlined that states were at all times obliged to peaceful settlement regardless of whether or not the dispute was qualified as an international dispute under UN Charter. However, participants reflected that there was still a lot of disagreement on the interpretation of the PSD obligation. For example, it is unclear when a State would be breaching the obligation. It was also discussed whether the PSD obligation was limited to cases that endanger peace and security, and how to determine reaching such a threshold. It was also discussed whether there would be a different assessment depending on the obligation, which was breached by the responsible State (referring to obligations *erga omnes*, multilateral treaty obligations, bilateral obligations, etc.).

The session included a substantive discussion on what is a dispute in the context of the UN Charter. For example, would all kinds of disputes go under the obligation of dispute settlement? One view was that a dispute needs to have a legal character, referencing ICJ jurisprudence. Several participants shared the view that a dispute does not have to necessarily entail a disagreement about legal matters such as whether or not a certain cyber operation qualifies as a wrongful act under international law. At the same time, it was suggested that a disagreement about legal matters could certainly be viewed as an example of a dispute, whereas other disagreements may not necessarily be viewed as disputes in the UN Charter context. In the latter category, the example of purely political disputes and therefore their status as “disputes” under the UN Charter was brought up and discussed without reaching a conclusion. There was yet another view according to which a dispute that should be solved by peaceful means is a dispute that cannot be solved through negotiations.

Many participants raised questions about the interpretation of the wording of the UN Charter. E.g. “*continuance of which*” – in Article 33 of the UN Charter (“*The parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security...*”) – does this mean that the dispute itself at that given moment does not necessarily have to endanger the maintenance of international peace and security but rather refers to a possible escalation? The usage of the term “*any situation*” in the UN Charter (e.g. Article 34 and Article 35) was also brought to the attention of the participants as possibly entailing a much broader meaning than a “dispute”.

There was a general agreement between several participants that the question of whether there is a dispute (or international dispute) depends on several aspects, including the accompanying elements of the behaviour of the States.

Several participants pointed out that mere statements (e.g. a tweet) are not disputes, as there is a tendency to be speaking about other States without engaging with them. It was added that the silence of one State does not necessarily indicate disagreement. Instead, silence may be necessary to finalise investigation or gather further information. However, it was noted that silence should be viewed together with the principle of good faith. One example of jurisprudence was also mentioned in the context of when silence could be regarded as opposition, thus creating a dispute.²

Some participants asked whether it even matters if the situation could be described as a dispute and wondered about the merits of the PSD obligations. Other participants pointed out that disagreements could also be solved by ethics, due-diligence and good will.

It was noted several times that attribution to a State is also required, but that it remains challenging. Different elements of attribution and information exchange (such as CERT-to-CERT) were elaborated upon. For example, victim States might not want to take to more formal mechanisms, or might not want to disclose what they know. As a practical example, one participant mentioned that some States do not want to devote the outcome to a third party, and may therefore resort to countermeasures. It was also suggested that a State could quickly go with public attribution (which may come after private); however, it should be kept in mind that this may be aggravating the dispute. On the contrary, such behaviour may encourage more serious negotiations.

One participant noted that there is an obligation to raise it privately that there is a dispute, also to point out a lack of good faith (otherwise PSD can wane). In such cases, there is a chance that the affected State considers other tools.

One participant wondered about the link between State-sponsored operators (e.g. criminal groups) and the obligation for PSD.

3. **What is the role of good faith in PSD?** The relevance of good faith in the relations between States was underlined on numerous occasions. It was also noted that it is challenging to operate in circumstances where one actor does not have good faith. The refusal of listening to the opposing party's arguments was cited as an example of lacking good faith. One participant pointed out that in the context of good faith it was also relevant to distinguish between lack of willingness and lack of ability.
4. **Employing PSD in practice.** Several participants raised the question of the actual employment of the PSD in practice in relation to cyber operations, as the PSD mechanisms do not seem to be the first resort for States when looking at real cases. One participant suggested that the interpretation of PSD needed to take into account the context and history of the obligation, referring to the systemic integration of the rules.

Some participants reflected that currently there was more focus on good faith and due diligence than on implementing PSD. One reason for this may be that the issues related to cyber require quick responses and in cyber, States tend to prefer shortcuts to following the traditional ways of negotiating and discussing. It was also discussed whether other countries have the right to assist States in fulfilling the PSD obligation.

The obligations of the parties of the dispute were also under debate. It was generally accepted that there is a general agreement that an international situation has to be managed peacefully.

² Republic of Ecuador vs USA <https://www.italaw.com/cases/1494>

It was also generally agreed that parties do not have to resolve the matter since forcing parties to the table may cause more trouble. It was iterated that there may be circumstances where doing nothing can be the right course of action.

Several participants confirmed that there is an obligation to raise concerns to the offending State (i.e. the injured State should speak out), either privately or publicly, so that there is an obligation to notify of the injury.

In relation to PSD, the topic of due diligence also came up. It was reminded that due diligence means taking all feasible measures within the capacity of the State. Several participants underscored that an incapable State (willing but not able) cannot be the target of countermeasures for breach of due diligence. However, unwillingness (yet existing ability) would be considered a breach of due diligence.

5. **What is peaceful? Are countermeasures peaceful?** Several participants were puzzled as to whether countermeasures could be part of the PSD. Several participants agreed that countermeasures are peaceful since they are a legal tool available for States, and part of the PSD, and can also be viewed separately as a distinct measure. It was underlined that countermeasures are lawful under certain conditions, and that countermeasures should be aimed at ending or limiting the dispute. One participant noted that in practice countermeasures are considered when the aim is resolution instead of escalation. It was shared that some countries may be adamant against PSD because they do not want to become the target of legitimate countermeasures.

Several participants also mentioned the element of notification/notice and asked about the correlation to PSD; one participant stating that it was a prerequisite. It was noted that the notification requirement may not be well suited to the cyber environment, and it may also render countermeasures ineffective (e.g. the target can prepare). Another participant mentioned that notification of countermeasures is not a requirement *per se*, but rather a State generally needs to call on the offending State to cease its wrongful conduct. It was also asked if a State carried out countermeasures covertly, how would the injured State (i.e. the target of the countermeasures) know that these are actually countermeasures?

One participant argued that countermeasures may be seen as peaceful, but may also bring along yet another dispute if the other State disagrees with the legality of the countermeasure. It was noted several times that the use of force would not be considered as peaceful.

6. **The role of collective countermeasures in PSD.** There are different views on collective countermeasures. Some participants mentioned that there are countries that are not ruling out collective countermeasures. One participant added that there was a tendency to move towards employing collective countermeasures in practice. Several participants suggested that a joint response could be more effective than the response of a single state. It was recalled that there is a difference between collective countermeasures and coordinated countermeasures.

One participant referred to the Draft Articles on State Responsibility and reminded that States may look for assistance, but the rights are held by the injured state and there are several obligations arising from them, including that the countermeasures need to be proportionate, etc. Another participant put forward the view that countermeasures require the State that employs them to be a victim of a wrongful act and therefore others who are not a victim cannot legally perform what would at that point be a wrongful act.

It was then discussed whether it would be useful to separate “assisting” the injured states from “conducting countermeasures” on behalf of the other State. So that even when rejecting the option of collective countermeasures, some States may accept assistance that would not violate an obligation owed to the responsible State by the assisting State (like respect for sovereignty) because there would be no grounds for the preclusion of wrongfulness.

A question was raised whether a State needed to be a party to a dispute if the State was taking action under that rule? Along the same lines, it was discussed whether it was the intention of the ILC to allow an unlimited number of States to respond by actions that would otherwise be unlawful (related to collective countermeasures). This raises the question that if multiple States respond to a wrongful act by one State, are all those multiple States now parties to a dispute, and thus subject to the PSD? And would this then serve the purpose of de-escalating disputes?

- 7. The role of the ICJ and the Security Council in PSD.** It was suggested that States should use available legal tools as prescribed in documents such as the UN Charter. These include referring a case to the UN Security Council (SC), such as under Article 37 of the UN Charter if the Article 33 process does not resolve the dispute, or going to the ICJ. However, several participants underscored that there is no obligation to go to the ICJ or SC or other options proposed in the UN Charter. These should be viewed as paths along PSD or as part of PSD. Some States have underlined the importance and role of the UN SC in the matter. A concrete example was cited of an initiative tabled by Senegal and Spain that was brought to the attention of the UN SC in 2016. Questions were raised about the ability of the ICJ to consider attribution and context.

There was no agreement on the role of the SC. However, an observation was made regarding the equality of the parties to a dispute if one party was a permanent member of the UN SC. The disparity stems from the veto power of permanent members as defined under Article 27 (3) of the UN Charter. Despite the caveat that the veto power shall not be used by a party to a dispute under Chapter VI and Article 52, the argument could be made that if a dispute escalates from under Chapter VI to Chapter VII (Actions threatening peace) this enables the veto to be used again. As such, Article 36 under Chapter VI only allows for “recommendations”, whereas Article 39 under Chapter VII enables decisions as to e.g. sanctions (Article 41) or even military force (Article 42), thereby the veto can be used to block more concrete measures. This connected with the debate about the status of remaining silent when engaged in a debate. It was suggested that permanent members of the UN SC could under the above-mentioned terms benefit more from such a tactic as even if there was an escalation they could formally utilise their veto to block concrete consequences from the SC. This is a benefit not available for States that are not permanent SC members. However, it was pointed out that such manoeuvring would come at a significant reputational and political cost.

1.3 Sovereignty

The foundations of the principle of sovereignty were introduced to the participants. The difference in views — such as seeing sovereignty as a standalone rule or as a mere principle — was explained. If sovereignty is viewed as a rule, then the States should further elaborate upon its content. One participant noted that if sovereignty is viewed as a principle, it is easier to determine a violation, whereas if it is considered as a rule, more precision is needed. The following issues were discussed.

- 1. Thresholds for breaching sovereignty.** Participants who viewed sovereignty as a standalone rule had different views on the thresholds.

There were participants who expressed the understanding that remotely accessing the networks and infrastructure of another State with a malicious intent entails a breach of sovereignty. For others, merely accessing the data seemed too low as a threshold for breaching sovereignty. The threshold of loss of functionality was also discussed, as this appeared as a certain breach for some participants. Another view links the threshold with causing effects on the territory of another state without consent (deriving from the logic that States have the right to control what happens on their territory).

Questions were also raised about whether installing malware entails a breach of sovereignty. One participant pointed out that if the malware is installed but not activated, it is not clear whether this entails a breach of sovereignty – in other words, it is not evident whether the assessment should also take into account potential consequences or the type of malware installed.

Another participant raised the issue of intent and purpose. There may be a situation where there was a concrete purpose (e.g. to stop the system from operating normally) but the IT security came in and stopped it. Can we then talk about an attempt or a threat – such as the threat to use force? Also, as discussed before, there may be a breach, but the State is unaware of it and cannot do anything.

On the issue of preventing access to databases, several participants stated that this may be a breach, but more information on the operation and its effects would be needed.

One participant suggested that the cyber sanction regime criteria (cyberattacks with potentially significant effect) should be considered and that this could be used for discussing *de minimis* threshold.

Additionally, the applicability of national law was emphasised, and how it could be used instead of or in parallel to international law. It was shared that national law may be better suited to deal with less intense cyber operations, even when carried out by State actors. It was argued that from a certain threshold – such as targeting government databases and making them inaccessible for the government – the operation could be viewed as a breach of sovereignty.

- 2. Exercise of governmental functions.** It was asked if sovereignty protects the exercise of governmental functions, then which functions are these? If governmental functions can be contracted to the private sector, can these then also be viewed as a breach of sovereignty? Several considerations were outlined, for example, the motivation of the attackers and whether the attack was intended to cause harm specifically to a certain government. Similarly, the point was raised that in practice an attacker may not even be aware of the services a private company is providing to the government and as such, any damage to the State is unintended. Moreover, the role of the private company was raised, whether it was providing an inherently governmental role, which could therefore be usurped or interrupted by the attack. Discussions touched upon the content of the contract between the State and the private entity and whether the private entity can be seen as exercising public power. The meaning of usurpation was examined. However, several participants reiterated that a State-sponsored operation against a private sector can be viewed as a breach of sovereignty and the status of the contractor does not matter.

A parallel was drawn with a private entity who is physically guarding a State government building. A participant shared that getting through the physical defence (interfering with the private entity in charge of the physical protection) would be a great concern with a more serious response. Another participant agreed that it was easier to make the assessment in more “kinetic” circumstances since the website defacement case seems more intangible, more technical and difficult to assess. States should discuss and formulate interpretations.

3. **Interference with inherently State functions.** It was discussed what does an interference with inherently State functions entail. For example, would undermining performance or confidence be interference or disrupting the delivery of an inherently governmental function? It was reminded that the legal assessment should take into account both the violations based on territoriality as well as those based on interfering with inherently governmental functions. A remark was made that the notion of “inherently” suggests it is a function that all governments perform; otherwise, the right of sovereignty would vary from State to State.
4. **Defacement.** In relation to the defacement of websites, the classification of the consequences was questioned, whereby even if the defamation was seemingly minor or localized, would the rest of the website be reliable on and therefore perform its governmental function? Some participants questioned whether defacement could be seen as disruptive enough to entail a breach of sovereignty. One participant also noted that if part of a larger campaign, the episode of defacement may also be a breach of sovereignty. The context of the defacement is also relevant, e.g. whether it is conducted amidst an armed conflict.
5. **Territoriality in cyberspace.** The aspect of territoriality was also mentioned by several participants. For example, the parallel of physically entering the territory of one State was compared to remotely gaining access to the information systems of that State. The view of several participants was that the first episode in the scenario, where the agents of State A entered the territory of State B, constituted a breach of sovereignty. The reasoning included the notion that deciding who may cross the border to enter the territory is considered a fundamental part of sovereignty. However, there was also a view that cautioned that more information is needed on the purposes of the activities of the agents of the other State in order to qualify such physical entry as a breach of sovereignty. One participant underlined that the mere presence of the agents of one State on the territory of another State does not entail a breach of sovereignty. Another participant concurred and suggested that the case should be dealt with by national law. It was also suggested that both international law and national law can be used in this case.
6. **Intent.** The importance of intent was raised in relation to violations of sovereignty, such as if an aircraft becomes lost and accidentally violates the airspace of another country by entering it without their consent and whether such incursions would amount to a violation of sovereignty. A similar situation is an unintentional use of force. There was no consensus on the element of intent in regard to sovereignty.
7. **Political and strategic implications.** Several participants brought out arguments related to political and strategic elements, which should be taken into account when assessing particular cases. It was underscored several times that the legal assessment should not be viewed in isolation.
8. **Remote law enforcement operations.** Participants agreed that international law remains unsettled as to whether remote searches can be viewed as interference with inherently governmental functions such as investigations. Several relevant elements were mentioned. Firstly, publicly available data can be accessed remotely with no legal issues raised (see also Article 32 in the Budapest Convention). Equally, it may be argued that law enforcement operations targeted against malicious activities undertaken in the darknet do not include a breach of sovereignty because they are meant to be accessible outside the confines of the State.

One participant explained that remote investigations should always seek to employ the Mutual Legal Assistance process in order to ensure the admissibility of evidence in court. The participant continued that if another country would conduct remote investigation on their territory, this would be viewed as a violation of sovereignty. An example of the antitrust case

investigation by the USA was brought to the attention of the participants. Another participant mentioned that it is also relevant to assess the particular circumstances in cases where, for example, the investigated individual is the citizen of the State that is carrying out the investigation even if that individual (and the data that needs to be accessed) is residing on the territory of another State.

The element of “loss of location” or the “loss of knowledge of location” was discussed. The technological development and difficulties in determining the (physical) location of the data were acknowledged as adding to the challenges related to conducting criminal investigations. It was asked whether the loss of location could be seen as precluding the wrongfulness of the remote criminal investigations. One participant highlighted the technical complexities related to determining the location of the data and being able to be sure about whether such access to data would bring along an impact or an effect. The participant wondered how States could even learn about the impact or effect if they do not know where the data is (e.g. in case of transiting data). It was noted that an interesting legal situation would occur: we may assess that a remote investigative measure violates sovereignty, but because of the lack of knowledge about the location of the data, we cannot determine whose sovereignty was violated. One participant indicated that in practical terms, if a State does not know data location but is able to access the data within its jurisdiction, there is no violation of international law. However, if the physical location of the server becomes known, then permission from the other State should be asked. Examples of national provisions were shared.

The discussion then moved on to the element of good faith in remotely accessing data and determining the location thereof. A participant suggested that the good faith argument can be raised and if the State is unaware of the location of the data, they are not consciously violating sovereignty. It was proposed that the fact that the State on whose territory the data is located is unaware of the operation should not matter in the legal assessment — it should still be considered as a breach of sovereignty.

There was also a discussion on when a State has taken reasonable steps to determine the loss of location — what should be the standard? Also, several States may be involved simultaneously, and this will add to the complexity of the assessment. One participant mentioned that in these circumstances the interpretation of international law should favour providing grounds for effective law enforcement and fighting crime. At the same time, another participant called for a balance between the effectiveness of operations and the violation of sovereignty.

Finally, several participants reminded that States should be more open in sharing their interpretation of international law in this context and try to bring more clarity to the current situation.

9. **Espionage.** The complicated relationship to espionage was discussed, with references made to a situation where the cyber operation does not bring along any harm to the system itself. It was mentioned that in practice preserving the value of the intelligence is higher if the adversary does not know its systems are possessed by the other side. In general, there is a reluctance by States to share further views on this, owing to the importance of espionage to them. It was underlined that international law does not prohibit espionage. However, the ways in which espionage operations are carried out may be wrongful under international law — e.g. covering tracks that cause physical damage to the system.

1.4 The principle of non-intervention

The principle of non-intervention was introduced. It was affirmed that the essence of intervention is a) use of means or methods of coercion, and b) interference with internal or external affairs (*domaine réservé*). The linkage between sovereignty and intervention was touched upon, and an argument was made that intervention is not necessarily a more severe, but a different violation than violation of sovereignty. Some participants also pointed out challenges related to the stability and predictability of the legal concept. A number of related issues were discussed.

1. **Coercion.** The participants discussed the meaning of coercion in cyberspace. There is a general understanding that coercion involves a demand “do X (or don’t do X) or else Y happens”. In cyber, there can also be another interpretation: to take choice out of one’s hands – make it impossible/take away the ability to make a choice; but there were also participants who were unsure whether the latter would entail intervention.

Some participants raised the issue that in practice the demands may not be quite as evident. There was some discussion about whether, if the different operations can be seen as a larger campaign, the initial demand expressed in the first episode could be seen as being applied to the following operations. It was also suggested – in the context of (mis)information campaigns – that a certain reaction from the population does not necessarily mean that the State was denied a choice to decide one way or another.

Also, it was unclear for participants whether undermining trust in the government or in democratic structures involves the element of coercion. Equally, questions were raised regarding the required level of coercion in a situation where a cyber operation is spreading true information, yet still undermines the incumbent government e.g. winning the elections. Or, would the assessment be different if the target State is able to withstand coercion, and no effects follow.

Several participants focused on the damages or results of the operation. For many, this is a factor that may need to be considered when classifying the coerciveness of the actions as well as whether the incident rises above the *de minimis* threshold. At the same time, there was another approach according to which spreading panic may be enough to constitute coercion or a breach of sovereignty.

Participants also mentioned the requirement of a causal link between the coercive action and the affairs of the State.

The possibility of lowering the bar of “coercion” was discussed on several instances. It was argued that even if the bar for coercion was lowered, the *domaine réservé* element would still need to be satisfied.

One participant cautioned against focusing too much on definitions and reminded that international law is constantly developing and legal assessments depend on various elements and interpretations.

2. **Coercion and influencing.** The view was also raised that coercion should be considered distinct from influencing, as otherwise, for example sanctions could be considered coercion. Under this view, influence without a purpose could not be considered coercion. Rather, coercion is about making (leaving them with no other choice) a State do or not do an action. The view was also expressed that the operation does not need to be successful to be considered coercion. However, it was underlined that in certain circumstances it may

be difficult to differentiate between influence and coercion. One participant suggested that the more one State controls the actions of the other State, the closer the situation is to intervention. One participant pointed out that just because a State feels it is coerced does not mean that it objectively is so. Therefore, there needs to be a case-by-case assessment to find the thin line between influence and intervention.

3. **Intent.** It was discussed whether the cyber operation needs to include an intent to be coercive. How to assess a situation where the operation is aimed at extorting money from private companies, but consequently the State revises its security? Another example was cited about elections: does the malicious actor have to succeed to such an extent that their preferred leader is elected, or is just interference enough?
4. **Domaine réservé.** Participants exchanged views on the scope of the concept. It was discussed which obligations fall into the *domaine réservé*. There was a consensus that healthcare belongs to the *domaine réservé*. The scope of *domaine réservé* can differ across States and at the same time, States' own *domaine réservé* may change with international legal obligations. It was explained that the *domaine réservé* and inherently governmental function are not the same, yet similar. Participants discussed whether human rights fall into the *domaine réservé* and whether countries have a concurring view on this.
5. **Linking demands and events.** Several participants underlined the potential for confusion in a real-life situation where there may be a presumption that events occurring are all connected to one another, and thereby misinterpretations may occur. Moreover, the issue of considering events that by themselves would not amount to a violation, but taken together they could amount to a violation was additionally raised in this context, which emphasises the importance of having a clear and accurate understanding of which events and demands are connected (which may not be the case in real life). Attributing between cause and effect was also emphasized.
6. **Attribution.** Participants additionally discussed attribution, whereby a distinction between political, technical and legal attribution was mentioned. In essence, States may be reluctant to press forth with legal attribution in a forum that would require the disclosure of their technical capability in attributing the action. Consequently, some States prefer political attribution to ensure their technical capabilities remain hidden.
7. **Policy and strategy.** Policy and strategic elements and objectives were underscored in several instances. It was suggested that more information on these would facilitate the legal assessment and that there should be a balance between legal and policy arguments. In the context of developing a vaccine, ethical implications were also mentioned.

II Tallinn Workshop on International Law and Cyber Operations, 6–7 June 2022

The following summarises the discussions of the II Tallinn Workshop on International Law and Cyber Operations, held in Tallinn on 6–7 June 2022. The workshop included presentations and discussions led by Professor Dapo Akande (Oxford University) and Professor Scott Shackelford (Indiana University). All discussions were held under the Chatham House rule. The summary includes references to the scenario-based discussions held during the workshop.

2.1 State Responsibility (legal focus)

After a welcome by the representative of the Estonian Ministry of Foreign Affairs, the first session focused on state responsibility. After a comprehensive overview of the subject (slides are available), more detailed discussions were held in the plenary as well as in the breakout groups format. The topics included:

1. **State organs.** Participants discussed the foundations of state responsibility and determining whether there are grounds for attributing an activity of an entity to a state. Different options were discussed, such as examples of a state organ, a *de facto* organ, or a non-state actor acting under the direct control of a state. Issues related to a “direct link” were raised. It was suggested that if it can be proven that the entity is a state organ, attribution would be easier as the state is responsible for all their actions.

It was also discussed whether the organs of one state can engage in an action that is attributable to another state. It was suggested that in the case of armed forces, it would be unlikely that the armed forces of one country would be subject to the exclusive direction and control of the receiving state. This issue has arisen in the context of military operations, when the members of the armed forces are embedded in another state; however, as a rule, full command is not transferred.

For example, in the Tallinn Manual, if you have members of the CERT of one state that are put at the disposal of another state and they are asked to respond to incidents, it might include a scenario where the CERT’s actions are attributable to the other state provided they are under the exclusive direction and control of that state. Such a scenario would require that the CERT is acting for the purposes of the receiving state rather than the sending state.

2. **Assistance.** It was underlined that by providing aid or assistance, State A could bear international responsibility for the wrongful actions State B has been conducting.
3. **State authority and exercising state functions.** There was a broad discussion on which activities fall under state authority. Participants gave examples such as collecting taxes,

security and law enforcement. Cloud services were also discussed and it was asked whether using cloud services for the purpose of collecting taxes, e.g. for retaining tax-related data, could be seen as exercising governmental authority. There were different views on possible interpretations, depending on the circumstances; one of the main discussion points being whether retaining data can be viewed as a governmental function.

It was also mentioned that in real life the cases often have many entities involved and such a “chain of responsibility” (e.g. if it is not a state owned company that violates the international obligation but a sub-contractor) makes attribution even more difficult. It was argued that if a state is instructing or controlling a company, then the company becomes a *de facto* state organ and can also instruct and control. However, if the actions are attributed to the state by some other means, then you would have an additional layer of questions. These include, e.g. when that company gives directions or controls e.g. a sub-contractor, does it act in the form of a governmental authority or on its own? This would mean that the scope for finding the connecting link is narrower, whereas if it is an organ under the draft Article 4 on State Responsibility, all of its actions are attributable to the state. In general, it was observed that such a chain should in principle not hinder the attribution.

4. **Ultra vires.** It was discussed whether the actions of a state organ or a *de facto* state organ that have been conducted outside the power of the state could still lead to state responsibility. A hypothetical scenario was shared: a *de facto* state organ, which is completely dependent on the state, gathers information under the instructions of that state with the purpose of disrupting elections in another state. Now, the *de facto* state organ suddenly decides to employ ransomware (without such instructions being given from the state). The question then arises whether the *de facto* state organ has acted in its official capacity. It was suggested that there may be cases where even if the act was *ultra vires*, the state could be held responsible.

There was general agreement that in cyberspace it is very challenging to determine whether an actor has acted in their official capacity or not. Several participants suggested that circumstances may provide more hints such as which tools were employed, the use of uniforms /official premises, patterns of actions and the action being driven by an individual or the whole group/entity. Some participants also made references to the due diligence obligation of states. One participant also mentioned Law of Armed Conflict, AP I, Article 91 which states that the state is responsible for all the acts of the armed forces, and it was discussed whether the concept of *ultra vires* is approached differently under armed conflict.

5. **Adopting actions.** Participants also raised the question of whether the glorification of an individual’s actions by a state (e.g. after the acts have been committed), expressing support for the operations on e.g. the official website or knowingly agreeing to the operations may lead to state attribution. Several participants discussed whether an action can be adopted before the cyber operation it actually takes place. A participant noted that in the case of the particular scenario discussed during group work, there is no evidence about the state condemning the cyber operation at a later stage, and we know of no attempts to hold people responsible for their actions, which may offer support for establishing state responsibility.
6. **Control, directions, instructions.** Several participants agreed that proving the requisite control, directions and instructions may be very challenging. The participants were reminded that “control” is a high threshold and entails not just control but complete dependence on the state is required, so that this entity would not exist but for the state. However, the interpretation of “direction” and “instructions” is much more nuanced. Based on the scenario, the groups discussed whether approving the buying of malware

specifically designed to target a certain entity would entail “directions” or “instructions”. It was also asked whether “direction” is enough for establishing state responsibility. Views on this differed. Several participants needed more details to make an assessment, while others reminded that in “real life” there are often circumstances where an assessment needs to be made based on scattered evidence.

Several participants were wondering how much, in the case of the scenario, the company IkejaForce worked on its own, given that it already had its own tools and the scenario did not imply that the company was instructed by the state at all times. It was debated whether in order to establish attribution we need evidence of the state instructing and directing the whole operation, or only parts of it.

There was agreement that in practice it is very hard to demonstrate the state’s control and knowledge about an operation in order for the state to be considered responsible for it. One participant pointed out that unfortunately, there are no textbook cases in real life.

7. **State ownership.** There was a general agreement that if a company is state-owned, this does not necessarily mean that the state is responsible for the company’s actions. In the context of the scenario it was generally agreed that more evidence is needed that the state used its ownership in controlling the way the company acted; this may also depend on what is the purpose and function of the company. However, it was pointed out that this can vary between states as in some countries state ownership may imply greater control.
8. **Identifying actions and intent.** With regard to the scenario, all groups discussed the distinction between the purchase of the worm and its deployment. It was underlined several times that it is relevant to identify a wrongful act under international law. There was disagreement whether merely buying a highly specific malicious cyber weapon could be interpreted as a wrongful act. There were different views on this, e.g. whether this could be viewed as a threat of use of force. Possible treaty obligations must also be taken into account. Some participants suggested that the mere purchasing of malware may not be wrongful as there may be legitimate, e.g. defensive uses. It was also debated whether an agreement to buy the malware entails the agreement to deploy it; how to determine who made the decision to buy the malware; and whether the consequences of such an approval were acknowledged. Yet, there was a viewpoint that the distinction between the purchase and the deployment of the virus is not relevant, as it could be interpreted from the known information that the aim of the purchase was to use it for concrete targets.

The nature of purchases on the dark web was mentioned, and it was argued that as there may not be a contract, proving intent may be extremely difficult. It was discussed that even if there were a contract and it included certain clauses, this may not be regarded as “effective control”. Some participants also raised the question of a “shared goal” and its role in the legal assessment. Others pointed out that in the scenario Shiwa may have had the obligation to notify other affected states about the malware sold on the dark web.

Similarly, it was discussed whether the fact that there was limited or no cascading effect to the operation in the scenario, that is to say, the threat vectors/effects were tailored, bears any relevance from an attribution point of view. Others concluded that the effects were indeed cascading and unintentional. It was noted that the unintended cascading effects would suggest that the malware was not that specific after all, making it more difficult to identify the instructions.

More generally, the question was raised whether, in respect to the law of state responsibility, it matters if one can foresee consequences. It was put forward that unintended consequences do not matter that much for attribution, but might matter for the identification of the breach.

9. **Identifying patterns.** The importance of a consistent pattern, in the sense that the same non-state actor is suspected to be repeatedly used by a state to conduct cyber operations, was mentioned. As a corollary, if a non-state actor is used only once, it may be more difficult to attribute its actions to the state.
10. **Role of national law.** Participants also discussed the role of national law and international cooperation in responding to the scenarios, given the possible distinction of different acts. It was suggested that employing national law would be faster; however, there are several challenges, such as jurisdiction. The role of diplomacy was underlined as a useful tool in addressing cyber incidents.
11. **Evidence.** The thresholds for evidence were discussed on several occasions. One participant shared that there are ongoing discussions regarding what kind of evidence is needed in the cyber domain for the purposes of satisfying the “control” element. One viewpoint is that cyberspace should feature different types of tests for control/evidentiary standards because it is challenging to find similar evidence such as was the case of the Nicaragua judgement. Issues related to sharing the evidence and enforceability of law were also discussed.
12. **Due diligence.** Participants discussed whether we have a principle or an obligation of due diligence. Some participants put forward that in some cases, due diligence may be the best option to establish state responsibility in cyberspace.
13. **Damage.** Some participants underlined the importance of the discussions on the damage resulting from the cyber operations in question. It was suggested that damage matters in two principle ways. Firstly, it may be relevant to determine the costs of the malicious acts, e.g. for claims for reparations/compensation. Secondly, the impact matters in terms of the level of infringement, such as sovereignty, non-intervention or others. One participant mentioned that damage matters mostly from the political perspective.

2.2 Attribution (strategic, policy focus)

The second session focused on the strategic and policy aspects related to attribution. After the introduction to the topic (slides are available), several issues were raised.

1. **(Public) attribution.** One useful illustration was the “cake” approach, which helped to divide attribution into several phases. The political layer includes the political “boldness” to attribute, the technical layer is based on information needed, but measures and reactions require legal attribution. The EU cyber diplomacy toolbox was also discussed, highlighting that states have many options available for responding. It was repeatedly underlined that the circumstances of the incident need to be taken into account and there is no one-fits-all solution.

It was noted that a wrongful public attribution cannot be considered a breach of international law. However, domestic approaches were shared, such as the possible breach of the principle of the “dignity of state”. “Naming and shaming” as well as indictments were discussed and latest trends examined. It was underlined that good governance matters and attribution needs to be used sensibly, keeping in mind the factor of credibility.

One participant observed that public attribution may also be used to raise awareness about threats and warn the public, especially when the operations have targeted a public good. Another participant remained cautious about public attribution in the scenario, pointing out that since there was already an accusation by a private entity, the situation may escalate and

bilateral diplomacy or closed-door negotiations could be a better way forward. It was shared that the internal decision to attribute may come after big debates and there may also be situations where the decision must be carefully analysed as it could show certain weaknesses.

Another participant observed that public attribution should not hinder ongoing criminal investigations. It was also discussed whether the country that has been hit the hardest should be the one to attribute, or if regional organisations would be better suited for attribution in some cases. Yet, there was another view according to which the involvement of a greater number of states would lead to a bigger risk of the process becoming time-consuming and diluting the outcome to the lowest common denominator.

One participant expressed the opinion that public attribution may be the last step for a country to consider. Before that, the state should assess other options and consider different levels of attribution, including indirect attribution. For example, one can point out the malicious actor without attributing the activity to a state, possibly asking the state concerned to act.

Other participants underlined that the overall goal should be to establish what constitutes acceptable state behaviour. This means that if a state does not use the opportunity and fails to act in response to a malicious act, it may confirm to some extent that the state accepts such behaviour. However, the goal should be to avoid similar future activity.

In general, there were several participants expressing concern about the internal (domestic) exchange of views before attribution decisions are made (in other words: combining legal and political attribution) and called for the need to involve lawyers in such discussions at earlier stages.

2. **Private (sector) attribution.** Pros and cons were discussed. The pros include that the attribution may be quicker, the private sector may have more tools, and they may be useful in demonstrating that your state is not alone in attributing the incident. Private attribution also allows the government to point to something that is not classified, and this can be very convenient if the attribution is correct. One participant assessed that the private sectors' involvement in attribution is a game changer and a trend that cannot be reversed.

However, numerous disadvantages and potential risks were also mentioned, such as the trustworthiness of private attribution, which has to be evaluated individually. Also, private attribution may increase political pressure for public attribution. Some participants also pointed out that as the private companies are not recognized entities in international law, private attribution may reduce the value of the attribution from a pure international law perspective. Moreover, it was felt that states should be the ones making policy decisions, and should always conduct their own assessment and not rely purely on private attribution, as this was felt to be irresponsible and even potentially a breach of due diligence. Some participants pointed out that the governments need to make a careful decision over whether to mention that they have used private sector data for agreeing on an attribution. One participant underlined the possibility of the opinion of a private entity and private attribution being perceived as those of a state (e.g. the state where that private entity is based in), which is something that the state does not necessarily agree with. Some participants were of the opinion that hybrid attribution (public + private; or multistakeholder) may be successful.

Some participants also discussed the obligation of the private entity to share information about the incident with the government.

3. **Collective attribution.** Several benefits and risks were noted. Benefits included a "louder" message, mitigating the risk of being targeted in retaliation, since there are more targets to

pick from, and potentially even a more credible attribution as more states are convinced of the(ir) evidence. Some participants supported the view that when effects are manifested in both states, bilateral attribution is useful.

However, collective attribution may also dilute the effect to the lowest common denominator in order to reach a result acceptable to all. Consequently, it may be prudent to first begin with a smaller group of like-minded or close allies and then proceed to larger groups if collective attribution is pursued. In addition, it was noted that the law may be used as an excuse for not taking steps due to political considerations rather than actual legal problems. Another participant asserted that attribution matters if there is a coordinated response, otherwise it does not have an effect.

4. **Evidence.** Several participants highlighted challenges related to information sharing (e.g. regarding vulnerabilities) in the context of collective attribution, which can complicate attribution. While there was a general agreement that there is no legal obligation to share evidence, the participants had different opinions on how much, if at all, evidence should be shared. Some supported the view that some parts of the evidence can be shared, adding to the credibility of the attribution. Others warned against sharing too much, e.g. on how the evidence was collected. Participants observed that in general detailed evidence is not shared publicly; however, evidence may be shared in bilateral and multilateral formats, based on e.g. security agreements. One participant suggested that the amount of confidence in the evidence probably varies according to which subsequent actions the state is expecting. It may be impossible to have 100 % certainty in some cases. Internal due diligence is needed before taking action based on the evidence available.
5. **Deterrence.** Different aspects of deterrence were discussed, such as sanctions, their effectiveness, international law, deterrence by denial (hardening networks).
6. **Indictments.** The relationship between indictments and attribution was discussed. Some participants found that indictments take time and attribution should follow the incident more closely. Ideally, indictments support the attribution, but it can be difficult because of the diverging timelines.

As a separate issue, the discussion addressed indictments of foreign officials in circumstances where it is unlikely that the individual will be prosecuted. One participant underlined that there is a wide range of tools available in domestic frameworks besides indictments. Another participant reminded that the domestic criminal indictment is very different from attribution, which may be a political move.

7. **Norms.** The role of norms in the context of attribution was raised. It was reminded that legal and political attributions differ, and that the issue of attribution is broader than the legal assessment. Interference with the US elections in 2016 was cited as an example where the classification of the incident in terms of international law or norms was not shared (publicly).

2.3 Retorsions

The third session focused on retorsion. After the introduction of the topic (slides are available), several issues were raised.

1. **General concept.** It was discussed that retorsion is always by definition legal (legal but unfriendly acts under international law). So in other words, if it is not lawful (e.g. after the assessment of a court), it is not a retorsion. However, it should be understood that a specific

measure can only be classified as retorsion after a legal assessment of that proposed specific action has been completed, rather than relying on inaccurate general categories. In other words, general categorization does not answer the question if the measure is lawful, one has to look precisely at the actual measure proposed to take and measure that specific act against the applicable obligations (e.g. treaty obligations, etc.) one has. It was noted that there may also be specific limitations to retorsions, deriving e.g. from the law of the treaties, depending on the concrete situation. It may be argued that some limitations to retorsion may be derived from the general principles of law, e.g. there may be a limitation to retorsions in terms of time (temporality).

It is important to note that if consequences occur towards individuals, there may be human rights implications and/or violations. Also, it was argued that the possibility of individuals and groups bringing claims against the state (e.g. concerning human rights violations) increases compared to state-to-state interactions. Examples of sinkholes, honeypots and surveillance (e.g. the Big Brother case) were examined. Participants also discussed the legality of cyber espionage, raising issues such as the (il)legality of acts of espionage under domestic law and if/how this affects the legal assessment under international law.

One participant observed that from an analytical perspective, retorsion should not be conflated with any lawful conduct. It was suggested that retorsions warrant additional thought on specific areas and limitations.

2. **Sanctions.** It was underlined that the term “sanction” is not a useful legal concept, as it is too general. One has to look at the specific measures being taken as the term “sanction” does not say much about the legal obligations one may be breaching. It was highlighted that whether or not one’s actions constitute a retorsion depends on the specific measure. Several issues related to sanctions were discussed, such as whether a state can employ sanctions against a third state.
3. **Erga omnes obligation violations.** The participants discussed the relationship between *erga omnes* obligation violations and retorsions. It was generally agreed that a violation of an *erga omnes* obligation that is owed to the community as a whole entails a violation of international law, and thereby states have several response options.
4. **Jus cogens norm violations.** It was also discussed whether there can be an obligation to employ sanctions in relation to the violation of a *jus cogens* norm. It was noted that law of state responsibility deals with how to respond to serious breaches of a *jus cogens* norm, claiming that states have an obligation a) to not provide aid and assistance to the violator, and b) to cooperate and take lawful measures to respond. However, there are ongoing discussions on what this means in practice. Since it is expressed in the ILC draft articles on State Responsibility as an obligation, one could argue that there is an obligation. The relationship between the UN Charter Article 2 (5) was also analysed.
5. **Examples of retorsion.** Retorsion options include responding in kind (such as a lack of cooperation is met with a lack of cooperation when legal), public criticism, expelling diplomats, limiting diplomatic relations, withdrawal of diplomatic services, exclusion of cooperation or certain cooperation formats (e.g. specific UN bodies), halting the delivery of certain types of technology, trade bans for certain goods, restrictions on investment, freezing assets, etc.

In terms of potential cyber examples of retorsion, various ideas were suggested: denying access to servers, services or certain websites, targeting the flow of information (transiting), terminating cloud services, terminating technical information sharing, influencing the

functionality in ports' infrastructure (scenario-specific), stopping the sharing of exploit information, social media campaigns, banning certain services (e.g. related to propaganda), and sending emails to certain government officials or related entities. Blocking internet access or websites was a controversial issue, as some felt it violates freedom of speech and is otherwise politically undesirable, and as such did not receive a widespread endorsement from the groups.

It was discussed that economic sanctions and retorsion could be stronger if employed in a group/by a regional organisation. However, it was also underlined that agreeing on certain sanctions within a group is more costly and complicated.

Other response options such as website defacement, spamming and DDoS attacks were also discussed, reaching the more general topic of the threshold for breaching sovereignty.

Finally, the role of the private sector in establishing their own restrictions/sanctions was also mentioned.

6. **Human rights and privacy.** Participants were reminded that privacy under human rights law is complicated and there is no room for generalisation. Each case should be carefully examined and as there is no absolute prohibition, one can interfere with the right if it is not arbitrary and provided by law, pursuant to a legitimate aim and proportionality. The relationship between countermeasures and human rights obligations was also discussed, e.g. if countermeasures against a state can also affect the nationals of that state.
7. **Proportionality.** Some participants noted that due to the Russian invasion of Ukraine and the drastic nature of the crisis, tough retorsion measures have been taken; however, proportionality should not be forgotten nor the fact that the measures taken there are some of the most severe. Proportionality was mentioned in the context of retorsion to avoid unnecessary escalation. It was also underlined that different countries may require different types of retorsions, and proportionality should be considered. However, it was left open if proportionality is a legal or political obligation, and if any restrictions would apply in that regard. The importance of including a defined end point to a retorsion was mentioned as otherwise they may be difficult to remove after they no longer serve their purpose.
8. **Inaction/lack of cooperation.** In terms of the scenarios discussed, participants had different views on reacting to the inaction of the other state regarding assistance on a specific matter. Some suggested targeted sanctions right away, while other took a more prudent approach and highlighted that there may be reasons for the other state for not responding. It was shared that in practice, response times are long and formalities may either intentionally or unintentionally delay the response to the request, potentially indefinitely. It is important to establish whether inaction is intentional or merely part of the standard practice of that state when responding to requests, including delays or even the request "getting lost". Several examples related to privileges, immunities and resident diplomats were shared. In such cases, letters of protest, media pressure, and starting one's own criminal investigation were mentioned as ways of obtaining a response. In other words, for several participants, going to higher levels such as ministers to respond to inaction is preferred over immediate retorsion.

According to some countries, there is no clear interpretation for an obligation for due diligence; however, there are (legally non-binding) norms of state behaviour for containing the same content. Participants shared challenges in relation to the concept of due diligence such as some countries lacking the capacity to investigate.

Some participants found it useful to turn to domestic law to determine whether a specific act was criminal according to national regulatory frameworks. It was suggested that local authorities may have a duty to investigate if they have been notified of a crime. In the case of the EU and the Council of Europe, there are a number of regulations, including direct methods of notification and subsequent direct cooperation, so there is no need to go through ministries. The participants also discussed other sources for a general duty to cooperate, citing the example of the Rome Statute; but concluded that such an obligation does not exist as a matter of customary international law.

Participants also discussed whether if one country lacks the capacity to investigate a certain act, another state could conduct the investigation on the territory of that state based on its consent. Different viewpoints were expressed. Some participants noted that in their experience, countries usually do not prefer to allow the law enforcement of another state to conduct such investigations on their territory.

The concept of good faith and peaceful settlement of disputes was also raised. Among other issues, the participants discussed the meaning of “peaceful” and “friendly”.

9. **Food for thought.** Participants discussed the fundamental question of whether there is a law of retorsion or whether retorsion is just a description of a thing/group of actions. The question was left unanswered.

III Tallinn Workshop on International Law and Cyber Operations, 3–4 October 2022

The following summarises the discussions of the III Tallinn Workshop on International Law and Cyber Operations, held in Tallinn on 3–4 October 2022. The workshop included presentations and discussions led by Prof Duncan Hollis (Temple University, USA) and Dr Francois Delerue (IE University, Spain). The majority of the specific examples discussed in the report originate from the scenarios. All discussions were held under the Chatham House rule. The summary includes references to the scenario-based discussions held during the workshop.

3.1 Use of force

After a comprehensive overview of the subject (slides are available), more detailed discussions were held in the plenary as well as in the breakout groups format. The topics included:

1. **State practice in general.** Several participants pointed out that States may choose not to openly demonstrate their practice but, for example, share their legal assessments in a closed circle. Some suggested that for the activity to be considered State practice, the State must acknowledge and defend it as lawful, although others suggested that it would be sufficient for the practice to be known. There may be public attribution, but in many cases the text does not indicate which laws were violated and for which attacks, so in most of these cases the law is silent on the accusation. Participants agreed that there could be many reasons for silence, underlining that in practice much of the behaviour of States, when done with offensive or defensive objectives, remains covert. There was a suggestion that in the cyber context governments might be quite reluctant to take specific positions due to operational flexibility – not to exclude operations from its arsenal it might need itself in the future. One participant underlined that the point of rule of law is consistency – and this may be the reason why States do not want to express its interpretation in a domain that is developing so fast. There was an opinion that the Albanian case illustrates an example where there is a statement regarding a concrete violation of international law (aggression), however, followed by poor reaction. One participant suggested that if a State has no credible mechanism to react, it may be better to remain silent. Another participant wondered whether it is a good idea to bring legal arguments into the discussion at all if it is known in advance that this will reveal the weakness of the law (or its enforcement). At the same time, it was found that there is value in saying that these are the rules and they will be enforced eventually.

It was also pointed out that likeminded States are increasingly shaping the development of law by vocally stating their opinion on what is what. Often States are unsure, their public statements are driven by politicians in a hurry, whereas lawyers need more time and do not have the time to get the text ready for the tweet. Sometimes the mentality is that if we do not

identify a particular operation under international law, others will be making the law. Politicians are afraid of being restrained by what lawyers say. Also, it is often difficult to come to an agreement domestically. It was suggested that lawyers better do the hard internal work in advance to be able to respond more promptly in time of crises.

Also, it was discussed whether silence indicates an agreement or lack thereof. There was also a question raised about what is of greater value in the context of international law: an official statement or actual practice? There is also a larger question of when is there a duty for other States to respond.

2. **Use of force.** Participants shared views on how to interpret whether a cyber operation amounts to a use of force. The options of analogies and scale and effects were examined. It was asked whether the prohibition to use force is a standard or a rule, and what are the differences between such interpretations, if any. It was iterated that international responsibility applies both to rules and standards. It was suggested that differentiating between rules, standards and principles may be not so clear cut. One view is that principles are broader, decontextualized and general statements; standards are more contextualized and a rule is the clearest of the three. It was asked whether standards could be used to interpret whether rules are violated. One participant indicated that adding "reasonable" to a clause makes it more like a standard because it brings about a whole host of other circumstances. UN Charter Article 41 was mentioned as listing measures not involving the use of armed force.
3. **Threshold for the use of force.** It was generally agreed that the threshold of use of force requires physical destruction. However, several participants had different views whether physical damage is enough to conclude on the use of force, or should there be harm to human life. One participant underlined the relevance of a military element: if satellites were destroyed by a missile, there would be no doubt that it would constitute use of force. Another participant pointed out that dual use objects always have a military element included, and this is why the categorisation of objects/targets is important. It was underlined that one should also always consider what obligations and effect the qualification as use of force entails, and whether one is ready for that. Some participants asked how much does it matter if a cyber operation was a covert operation? It was argued that, in the context of the scenario, as the target State was not aware of the malicious code, the subject for threat of use of force is missing. It was expressed that if a cyber operation damaged the satellite that controls hospitals and had a severe impact on civil society through hospitals, this should be deemed an unlawful use of force.

There was also the viewpoint that even if we cannot determine if the cyber operation amounts to a use of force through the violation of sovereignty or the violation of the principle of non-intervention, the target State still has the right to take countermeasures.

The relationship between the use of force and aggression was examined. The debate over whether some uses of force can be seen as not prohibited as *jus cogens* was mentioned.

4. **Targets.** There was also a discussion on the possible targets of the use of force. It was analysed whether the target of the use of force needs to be defined by strictly territorial integrity or political independence, or whether it could be read more widely and apply to any type of target, e.g. satellites. It was reminded that the wording of Article 2(4) also includes "or in any other manner inconsistent with the purposes of the United Nations", which allows for a broad interpretation. It was highlighted that it does not matter if e.g. the satellite system is a military or private asset, the owning State has sovereignty over it. Some participants raised the question whether it matters if the target is critical infrastructure or a dual-use object. It was also discussed whether the setting (space) sets some specific legal boundaries to the assessments.

5. **Intent.** There was the question on whether a “mistake” could be viewed as a use of force, e.g. when the coders make a mistake and the result is a Stuxnet type of a situation. What is the significance of a “mistake”, “attempt” and “intent”? A discussion ensued on the role of intent and the due diligence obligation. An example of Stuxnet was discussed and it was asked whether the fact that the malware did not stay within the nuclear facility and resulted in global infection was an intended or unintended consequence. Objective and subjective elements were discussed. It was suggested that cyber operations may have primary targets (such as Ukraine in the NotPetya case), and indirect consequences. Others did not consider non-Ukrainian targets in the NotPetya case as secondary.
6. **Non-State Actors (NSA).** It was discussed whether a NSA or a transnational terrorist organization or such could engage in a use of force? The Tallinn Manual says no. The International Court of Justice (ICJ) says that an armed attack has to be coming from a State, but after 9/11, the Security Council (SC) and a number of States said that NSA could also commit an armed attack. Participants agreed that there are different interpretations regarding this (e.g. in cases related to ISIS).

Several participants were worried about the actual remedies against the illegal activities of NSAs. It was proposed that the usual remedy would be cooperation with the territorial State. Also, there may be other circumstances precluding wrongfulness, such as necessity. Necessity could be one of the mechanisms if the NSA was attacking essential interests. Necessity does not require an internationally wrongful act, including attribution to a State. In some cases, below the threshold of use of force, due diligence can be used.

It was also discussed whether instead of debating whether NSA can use force, the focus of the interpretation could be on whether a State is unwilling and unable. It was shared that to date, the doctrine has been used by one State and other States have stated their opposition. It was explained that the idea behind it is that a State harbouring a NSA is unable and unwilling to act against them, which gives ground for the victim State to conduct an action against these individuals. There was no agreement over whether the actions according to that doctrine would be escalatory or not. It was expressed that using the doctrine in the context of cyber operations may be more complex.

7. **Preventive self-defence.** It was shared that there have been some instances of preventive self-defence in the past and there are views claiming that such actions are valid, while others disagree. Participants did not come to an agreement on the point at which targeting a future potential threat could be justified as preventative self-defence. Different characteristics of the potential threat were discussed, e.g. does it need to be specifically against military capabilities or can it also be undermining capabilities more generally. It was also discussed that maybe the target State allows for strategic reasons for certain damage to occur in order to have the right to certain responses against the adversary.
8. The **timing** element was discussed at great length. In the scenario, when does use of force start – when they hacked into the chips and placed the malicious code, when the satellite exploded (without the knowledge of the cyber operation) or when the malicious cyber operation was discovered? This information is relevant for the response of the target, such as for countermeasures or pre-emptive self-defence. An example from practice was shared where major DDOS attacks are conducted in order to act as a smokescreen for implementing malware. The questions there is similar – does the use of force begin with DDoS or when the destructive malware has resulted in destructive consequences? The majority were of the understanding that use of force occurs at the moment of the explosion, but there was also the view that use of force occurred when the command line was inserted because the activation of the code was automatic. A parallel with landmines was proposed.

Some participants viewed the explosion as an armed attack. The analysis of the causal chain to the effect was underlined, especially in the part of the scenario with a plane crash after the disruption of the GPS system. How much is the perpetrator responsible for unforeseeable (accidental) damages? What is unforeseeable in this context? Some argued that the plane crash would be foreseeable damage. Others disagreed and claimed that such disruption in the navigation system does not necessarily always lead to plane crashes. Hence, there was a disagreement over whether the plane crash could be considered as a use of force.

A participant commented that we needed to remind ourselves to distinguish between theory and practice. It is easy to assess events in retrospect, but if you really discover a logic bomb that has not done anything yet do you think that could be considered use of force? It was asked whether planting the code could be viewed as a threat to use of force. The opinion was put forward that if the code is found it is a threat of use of force if it has had no effects, but after execution, it is a clear case of use of force. Participants wondered that if such activity is a threat of use of force, which response options would the target State have. It was shared that in cyber the way the code is written is important; if it activates automatically then it is more than just a threat.

One participant put forward that it is difficult to make the decision only based on legal reasoning and you also need to consider political arguments. Actions in territorial seas have so far not been considered use of force, but could these be regarded as threats of use of force? Could the North Korean secret tunnels be regarded as threat of use of force? As of when? When they became public? It is difficult to see that as the target State is unaware of the malicious code. One participant underlined that for there to be a threat there needs to be knowledge about it.

3.2 Countermeasures

The second session focused on countermeasures. After a comprehensive overview of the subject (slides are available), more detailed discussions were held in the plenary as well as in the breakout groups format. The topics included:

1. **Timing.** There were similar discussions as above regarding the start of the violation, as this would allow for the use of countermeasures by the targeted State. Regarding the scenario, there were various views on whether the breach was ongoing or had ended with the self-destruction of the satellites. When you find malware in your systems, is it reasonable to believe that there is more? Do you need to actually reveal the malicious code or is it enough to assume that there is one? If you do not find the code and the responsible State says that it has deactivated the code, can you believe it? There was a view underlining that once the malicious code has been deleted, the breach has stopped. However, there was another viewpoint, stating that one should also look at the implications. If these continue, then there are grounds for countermeasures. It was discussed that even if the breaching State can end using the malware, does this mean that it is able to discontinue its effects? Some participants believed that the breach continues for as long the malware is functional. There was also the view that as long as the offending State has not offered full reparations, it is in breach of international law and countermeasures tailored to that effect are lawful. It was also discussed whether the lack of awareness by the affected State of the source of destruction could affect the use of countermeasures. The participants stated that the affected State could use countermeasures when they find out about the unlawful breach. In the context of the scenario discussed, one participant argued that it would be reasonable for the victim State to continue applying countermeasures until they are confident that the offending State will not continue their activities. When the offending State notes that they stopped the activity, then countermeasures would have to stop.

2. **Attribution.** It was proposed that reasonability is the only reasonable standard for evidence in the cyber context, and a higher standard would make the attribution in cyber impossible. A participant shared that one does have to make the attribution for the purposes of countermeasures but one does not have to report it to the SC. It was suggested that the likelihood of some court or the SC discussing a case of certain countermeasures is very small, unless there is a blatant breach of law. The SC may also intervene if the injured State brings it to the attention of the SC, who can then decide on the legality of the countermeasure. There might also be a tendency to use retorsions instead of countermeasures as it is also up to the other side to qualify the situation.
3. **Conditions.** It was emphasized that countermeasures need to be proportionate, reasonable and legal; they cannot be punitive; and they must be aimed at stopping the violation of international law. Some participants found it difficult to see how countermeasures would not turn out to be punitive. There was no agreement on whether countermeasures would encourage further attacks. It was concluded that conditions for countermeasures are very complex and difficult to fulfil in practice.
4. **Summation and notification** was also discussed. Several participants echoed that they would probably make the summation but not the notification about countermeasures. Yet, it was added that in cyber the summation requirement is not absolute. It was discussed whether the summation has to be in a given form and whether it is similar to the form of notification. It was asked whether the summation could also be part of a notification, and several participants supported the practice of making these together in one step. One participant suggested that necessity could justify and give a “free pass” on summation.

Is it enough for a notification to say that the response will be proportional or does it need to be more detailed? There was an understanding among some participants that notification was necessary, but the level of detail is up to the notifying State. Notification should be reasonably detailed without details on the chosen countermeasure so as not to undermine that. Given that the countermeasure need not be in-kind, one viewpoint was that the notification may just be about the intent to use countermeasures without further details. How the countermeasure is implemented is up to the injured State. The notification does not have to be public, but can be made also bilaterally. One participant pointed out that without notification the other country may not even notice that they are being targeted with countermeasures. It was discussed whether notification could be part of the proportionality assessment. It was suggested that if the breach is ongoing through the continuing implications, it is possible to disregard the notification, but if you build your countermeasures on reparations only, it is reasonable to make the notification. Participants agreed that there is no point in making the notification if by that you reveal your means and methods of discovering the breach. Several participants pointed out that in cyber the exception from notification becomes the rule, pointing to circumstances of urgency. Several participants underlined that if the issue is urgent, a State should have the right to act, not the obligation to negotiate with the other country.

It was shared that as an armed attack is an international wrongfully act, the victim State may respond with countermeasures and also self-defence measures. The SC needs to be informed in case of use of force. It was argued that States may choose whether their response measures would be public (self-defence) or not (countermeasures).

5. **Assistance and collective countermeasures.** Participants generally agreed that in the kinetic world it is easier to differentiate between collective countermeasures and assistance. In cyber the difference is not so clear-cut. There was an opinion expressed that there

is no right to collective countermeasures as the right to countermeasures or the injured status is not transferrable; however, assistance is legal when asked for. On the other hand, it was examined whether theoretically in circumstances where there is a legal basis for self-defence, could collective low threshold measures be taken instead, referring to a line of argumentation for collective countermeasures. No consensus was reached. Some participants expressed the view that coordinated countermeasures could be possible. If collective countermeasures were not possible, they could be considered parallel countermeasures – individual but coordinated.

It was also asked whether a State can assist in taking countermeasures or would this then automatically qualify as collective countermeasures. Participants asked whether collective assistance is legal. It was discussed what is assistance, and whether, e.g. sharing intelligence would qualify as assistance. Several participants agreed that giving assistance through advice remains within legal frames. Some participants made a distinction between actually taking part in countermeasures or assisting another State. There was also the view that that the assistance of another country comes with responsibility and this constitutes a collective countermeasure. It was noted that doing things alone or collectively had an impact on the proportionality assessment. Using the analogy, participants raised the question that if States are all assisting Ukraine in the war against Russia, does this mean that all these States are collectively at war with Russia. It was pointed out that until there is a wide acceptance by State practice, it is necessary to interpret the UN Charter in a narrow way; to extend it would be harmful.

3.3 Self-Defence

The third session focused on self-defence and necessity. After a comprehensive overview of the subject (slides are available), more detailed discussions were held in the plenary as well as in the breakout groups format. The topics included:

1. **Armed attack.** Several participants noted the different thresholds for an armed attack and use of force, underlining that the use of force is the prerequisite for armed attack. Some participants pointed out that it would be unlikely for an armed attack to be happening fully in cyber but rather in combination with other (kinetic) attacks. The scenario was discussed as to find examples of an armed attack. Participants analysed the damage (destruction of satellites, spillover effect to third countries) and could not find a consensus whether the destruction of satellites could be viewed as an armed attack. It was asked whether the nature of the target, the cumulative effect of the cyber operation or the setting (outer space) would influence the legal assessment. In the case of the scenario, the target was a communication satellite that would also support military independence – does this qualify as critical infrastructure? It was noted that it is not important whether the operation was successful in reaching its objective, as even a missed missile could be an armed attack in kinetic outer space. One participant also raised the level of decision for the operation, e.g. does it matter if it was a general or someone much lower-ranking making the final call.
It was also discussed whether in some circumstances it may be of the interest to the target State to call the operation an armed attack to gain access to self-defence. At the same time, it was cautioned that such action may lead to escalation.

Finally, it was noted that legal assessment would also depend on the political situation and what was expected by the government.

2. **Conditions for self-defence.** Participants discussed the conditions for self-defence. It was iterated that the right for self-defence stops when the violation ends but it is challenging to

identify when a violation has ended. It was noted that if there is no information that suggests further attacks, the **necessity** condition is not fulfilled, and the victim State cannot act in self-defence. However, others emphasized that it is very difficult to be sure that no further attacks would continue. Others also noted that the necessity condition may not be fulfilled by PRO's response as it is not clear how this operation may be bringing an end to Bilund's activities. There were also participants who could see the criteria of necessity being fulfilled as the armed attack was assessed as ongoing.

It was also discussed how to assess **proportionality** in the context of cyber operations. For example, is it proportionate to respond to the destruction of two rockets with launching a missile against a civilian satellite and disrupting the GPS positioning which *inter alia* leads to death? There was no consensus on this. One participant suggested that the assessment is again related to the expected consequences of taking out a satellite. By actually affecting a system that is globally used by many countries, for both military and civilian purposes, there may also be a spillover effect to third countries and this may result in the self-defence becoming disproportionate. It was also expressed that if the effects of that self-defence were felt elsewhere outside of Bilund, the response would be unlawful immediately, as self-defence would only justify breaching obligations against the target State and not any others. In that context, it was pointed out that making others use your own infrastructure was a good way of protecting it.

It was shared by some participants that in the kinetic world, proportionality is sometimes difficult to attain and assess, and we should think carefully before expecting more precision in cyberspace.

When it comes to the use of the private company MaXX, some participants said that it was unnecessary and disproportionate. Other argued that the use of MaXX was necessary and proportionate until the cargo plane fell.

3. **Preventative/pre-emptive self-defence.** One participant suggested that "what-if" scenarios should also be taken into account, e.g. what if the malware was not discovered and more launches of satellites would have continued, resulting in self-destruction. This means that the injured State may not be certain that there are no further attacks/damages occurring. Participants also asked whether one might rely on one's right to self-defence on suspicion (which may not be correct in the end, and end up escalating the whole situation)? Many agreed that in cyber it is very difficult to identify when is the "last moment to act". It was explained that the legal assessment may take scale and effects, intent as well as attempt into account but there are different views on this; e.g. some would prefer to only focus on scale and effects. The 2018 US Cyber Defence Strategy was also discussed and some participants found it to be an example of pre-emptive self-defence or countermeasures. However, it was cautioned that such activities may be viewed by other States as a breach of sovereignty, depending on their national interpretation.
4. **Damage.** Similar elements of damage were discussed as in previous sessions. Foreseeable effects were examined and it was agreed that assessing what is foreseeable and what is not can be very challenging. Several participants agreed that in case of the scenario, the plane crash was an indirect effect, but the automatic self-destruction of satellites was a direct effect and that should be weighed into the legal assessment. Others argued that taking down the navigation system and the subsequent plane crash were clearly causally connected, as it should have been foreseen that the air traffic system also depends on the navigation system. The timing is also important, e.g. was it to be foreseen that there would be air traffic when the navigation was taken down. The cumulative element of damages was

discussed in the context of evaluating the threshold of damage for an armed attack. One participant suggested that in practice States never get to the armed attack level because cybersecurity capabilities are growing and therefore the defence of the States will not let it cumulate to that level.

The territorial element of the scenarios was analysed. There was a viewpoint that there can be two victims of an armed attack through the same act: the first one is an armed attack against PRO, in the second is against PRO and Runtsu because there are physical damages (forest fires) also on the territory of Runtsu. Others disagreed that the damage which occurred in Runtsu would qualify as an armed attack. Several participants pointed at the need to analyse the scale and effect (e.g. duration of the fires, how many people effected). The cumulative aspects were also raised: if there would be evidence of a concerted campaign, there could be an argument that together this could raise to the level of an armed attack. There was another viewpoint that it may be a bit problematic in practice to put too much emphasis on where the rocket landed and what was the final damage as with armed attack (and any other violation) the victim State needs to act fast.

One participant expressed that there is also a possibility that firing a rocket against civilian telecommunication might have been the only way to get the offending State's interest and make contact with them, in case they had been ignoring requests for talks with the target State.

5. **Collective self-defence.** Several participants agreed that if the legal assessment concludes that there was an armed attack against PRO and Runtsu then PRO and Runtsu may take collective self-defence measures.
6. **Conditions for plea of necessity.** It was discussed whether any of the States' responses in the scenario could be seen as acting under the plea of necessity. Several participants agreed that necessity could only be used to defend your systems in case of imminent peril and in the defence of essential interests. It is difficult to define essential interests clearly. Can essential interest also be something that occurs in the future — e.g. in the case of testing satellites for a future system? Participants agreed that necessity should have a high-level threshold to prevent its misuse. Several participants underlined that there needs to be a causal link between the offending operation and the response under the plea of necessity, and noted that in the case of the scenario the nexus may not have been there. It was put forward that given that fulfilling the condition of necessity in real life is so challenging, it may be viewed as a less practical option in practice. Some participants disagreed and viewed the criteria of necessity as a fairly malleable characteristic.
7. **Separate regime for cyber.** In the end of this session, the participants examined whether there should be a separate legal regime or thresholds for cyber. Some participants noted that lowering the thresholds for cyberspace may lead to diluting them in other domains, which might be a net loss in the real world. Others suggested that in practice there already is a separate legal regime for cyberspace. Several participants cautioned that the discussions should remain focused on how to interpret existing international law and not move towards a new legal regime. One participant added that in practice, no one is looking at cyber operations in isolation, so that it is dangerous, for example, to suggest that self-defence is different in cyber. It was underlined that further discussions are needed between States on how to interpret international law in the context of cyber operations and to develop a consistent approach, taking into account the uniqueness of cyber. There was also the opinion expressed that States must consider whether additional rules and clarifications are needed to successfully complete the necessary improvements.

IV Tallinn Workshop on International Law and Cyber Operations, 30–31 March 2023

The following summarises the discussions of the IV Tallinn Workshop on International Law and Cyber Operations, held in Tallinn on 30–31 March 2023. The workshop included presentations and discussions led by Dr Kubo Mačák (International Committee of the Red Cross) and Dr Heather Harrison Dinniss (Swedish Defence University). All discussions were held under the Chatham House rule. The summary includes references to the scenario-based discussions held during the workshop.

4.1 The notion of an “attack”

After a welcome by the representative of the Estonian Ministry of Foreign Affairs, the first session focused on the notion of an attack. After a comprehensive overview of the subject (slides are available), more detailed discussions were held in the plenary as well as in the breakout groups format. The following topics were discussed.

1. **Regulation under IHL.** As a general rule, IHL applies to cyber operations that have a nexus with armed conflict. It was shared that cyber operations that would not be qualified as attacks could nevertheless be regulated by IHL because of other rules, which do not refer to attacks. Examples include the constant care obligation (i.e., the duty to take constant care to spare the civilian population, individual civilians, and civilian objects in the conduct of military operations), rules on special protection, and rules on the seizure/destruction of property.

Rules of conflict qualification were also raised as we witness many cyber operations without a link with an armed conflict. It was mentioned that it is unsettled what does “resort to armed force” mean in the cyber context. It was expressed that if we define “attacks” too broadly, and if an attack by one State against another is understood to amount to a resort to armed force between those States, we risk interpreting many existing cyber incidents as triggering a situation of armed conflict.

The scenarios illustrated the legal assessment in case of multiple individual cyber and kinetic operations. Some participants regarded these operations as one large operation, which would eventually change the legal assessment of the earlier individual operations. Others argued that in some cases it may make more sense to keep assessing the situation as separate operations. In the scenario discussion, the majority of participants underlined that IHL would apply from the first episode (annexation) and onwards. Some participants also raised the issue of the description of the incident from the policy perspective as this may influence the final assessment (e.g. whether to downplay the situation, or vice versa). It was also pointed out that operations that invite you to violate IHL obligations are in itself violating IHL as they would not be in accordance with the belligerents’ duty to respect and ensure respect for IHL at all times.

Equally, as preparations for the operations started before the belligerent occupation, would such preparatory work also be counted as in violation of IL? Some argued that preparatory work does not count under IHL as there is a need for effects but others disagreed, stating, *inter alia*, that IHL encourages also the preparatory work to take precautions.

2. **Threshold for “attack” under IHL and damage.** The understanding of the “act of violence” (Art 49 AP I) was discussed; in particular, whether “means” or “effects” should be violent in order for the criterion to be met. Additionally, it was asked whether all damage/destruction would qualify as “violence”.

Regarding damage, there are different viewpoints as to whether damage must be physical or can be viewed as broader, such as the need to replace physical components, need to reinstall software, or any loss of functionality.

There was a general agreement that cyber operations resulting in loss of life or injury would qualify as an “attack” under IHL. However, one participant raised the question of what level of injury would suffice, or whether losing one life would automatically qualify as an “attack” under IHL. The participants also discussed whether injuries and death would be foreseeable damage when attacking the ID-card system in a country where it is crucial for the functioning of medical facilities.

On the other hand, there seemed to be an understanding that the exfiltration of data or penetration of data with no additional consequences should not be regarded as an “attack” under IHL. One participant also raised the question on how to qualify cyber-enabled information operations directed against the civilian population (e.g. propaganda, undermining support for the conflict, etc.). It was shared that there is a discussion over the level of deception that may be involved in such operations.

A discussion ensued about the “loss of functionality” — e.g. cyber operations disabling online banking — some participants were uncomfortable stating that this would be enough for an “attack”; others argued that because of the large scope of effects, it should be considered as an “attack”. The participants raised several case studies where the legal assessment was not that clear. E.g. circumstances where the computer system continues to function as it was supposed to, but the cyber operation has resulted in slowing down the original function because it is also at the same time clandestinely performing another function. Another scenario discussed a case of reduced functionality, which results in harm to civilians. One participant argued that if a cyber operation targeted the whole civilian population, this might be considered as an “attack”. Participants discussed whether the fact that the target would be critical infrastructure would have an effect on the legal assessment. It was pointed out that medical facilities have a special protection under IHL, so targeting them would be a violation of IHL.

It was generally agreed that the effects are also dependent on the profile/characteristics of the country, e.g. the level of digitalization. The level of digitalization also plays a role in understanding what the effects will be as this would dictate the foreseeable damage. Different views were also expressed on “reversible and temporary effects” and whether this would matter for the legal assessment.

3. **Military necessity.** The legal value of necessity was discussed and whether the principle of military necessity informs the entire body of IHL but does not create obligations above and beyond specific rules of IHL, or whether it also imposes limits beyond specific IHL rules (i.e., even if a cyber operation during an armed conflict is not prohibited by a specific rule of IHL, under this latter approach, to be lawful it must nonetheless comply with the principle of military necessity).

4. **Causality.** The discussion focused on directly and indirectly causing the outcome of the cyber operation; taking note that sometimes cyber operations may have cascading or reverberating effects. Participants made a difference between reasonably expected outcomes and random outcomes, but noted that identifying the causal connection may sometimes be challenging. There may also be circumstances where operations which can be reasonably expected to cause certain things do not succeed. This also raises the question of intent and how to prove it. Another issue is the foreseeability of certain results of an operation and the responsibility for such results. It should not be relevant whether the target is private or public sector, what matters is the nexus between the operation and an ongoing armed conflict. There was a general agreement that such situations must be assessed case-by-case, looking at the attack as a whole, but that there may be responsibility also with only intent but no actual results. The scenarios raised several interesting questions, including about temporality: e.g. when a disinformation campaign takes place before the occupation, would it constitute part of the “attack”? Another scenario was shared: a group of civilians is escaping hostilities, and the adversary interferes with their GPS in a manner that they are directed at a minefield; it was proposed that if the action removes the free will of the individuals concerned, this may be considered as an attack.

4.2 Objects: dual use and data

The second session focused on objects and dual use. After a comprehensive overview of the subject (slides are available), more detailed discussions were held in the plenary as well as in the breakout groups format. The topics included:

1. Distinguishing between **civilian objects and military objectives**. It was reminded that 99% of the military communication goes over civilian infrastructure. As a general rule, civilian objects are all objects that are not military objectives and one cannot be both. Several participants pointed out that first it should be decided if data is an object, and then whether it is a military objective. It was noted that cloud computing may be promoted for being cost efficient, but it does not seem to factor in the possible implications regarding IHL and dual use together with possible military effects. There was a recommendation to avoid co-locating civilian and military data which should be applied already in peacetime; also, a recommendation to employ systems that allow to identify the location of the data (e.g. when using cloud computing).
2. **Data as an object.** According to one opinion, data is not an object and therefore cannot be a military objective; only hardware components can be military objectives. There was an opinion that even if data is not to be considered as an object, it would still be protected under different layers of IHL (e.g. conduct of hostilities, special protections). It was pointed out that even if taking the position that data is not an object, the digitalization of objects should not diminish their protection. However, one participant raised the question that if data is not considered an object, how would it be protected if there is not an attack under IHL (asking whether this could be seen as a legal gap).

According to another view, data could also be seen as a military objective (e.g. different applications as military objectives) and keeping to the traditional strict requirement for tangibility/materiality could lead to unreasonable results. Some participants stressed that data should be considered as an object, even if does not neatly fit into the legal framework; and if it would not be an object, data would be stripped of protection under IHL.

But there were different views on whether we can equal all kinds of data as an object. Some participants pointed out that not all data could be considered as an object, and we should make a difference between e.g. “code” and “data”. Yet, others said that if we agree that some

data is an object, then how could we say that other data is not an object; thus all data should be considered as an object given that that interpretation enhances the protection of civilians during situations of armed conflict, which is in line with the object and purpose of IHL. A teleological approach was also suggested, claiming that all civilian data should be seen as a civilian object. Although there were some disagreeing voices, the general agreement after the group discussions seems to be that at least some types of data should be viewed as an object.

An alternative view was to not define whether or not data can be an object but to focus on the effects – what matters are the consequences of the attacks.

During the discussions it was also noted that code could be property as well as considered as a weapon. The recommendation to avoid locating military objectives with civilian objects was underlined again. One participant suggested that laws need to be updated.

Another participant underlined that the topic of categorizing data is also significant in the context of ongoing global discussions, such as the Additional Protocol to the Budapest Convention and the Russian proposal for a new treaty.

3. **Effects of the attack.** During the scenario discussions it was argued that concerning the episode with Paxton it was not relevant to ask if data is an object, because data was protected in any case by IHL (interference with a humanitarian organisation). This raised the question whether any interference, e.g. copying or leaking data, would be a violation of IHL? There was a majority view that there needs to be an effect for the activity to be illegal; some pointed out that this particular activity may be considered as espionage. Others suggested that, even with concrete effects, some operations with data e.g. leaking of data should be considered espionage. Foreseeable results were also discussed. It was also asked how to get over the “violence” threshold; and suggested that if the notion of violence is conceptualized via effects (injury, death, damage) then we do not have to prove that the means were violent. Equally, the relationship between loss of functionality and “violence” was raised.
4. **Specially protected objects.** It was shared that there are also specially protected objects such as cultural property (archives), objects indispensable to the survival of the civilian population, medical units, humanitarian organizations, installations containing dangerous forces and natural environment. In other words, the nature of the data may affect the level of the protection the data enjoys. Participants also discussed whether under such a specialized regime the protection would fall on the operation of e.g. humanitarian organization or on the data of the humanitarian organization.
5. **Characteristics of data.** Participants outlined several challenges related to data. E.g. precautions in attack: one would need reconnaissance in order to do everything feasible to verify the targets. There is also the challenge under the law of neutrality in the context of the cloud service as the targeted data may be located in another (neutral) state. Participants also discussed how data could be divided into different categories (e.g. code and content data) and how this may affect the legal assessment. It was also discussed whether it matters if there is only one copy of the data.

4.3 Categories of persons involved in hostilities during armed conflicts

The third session focused on the categories of persons involved in hostilities during armed conflicts. After a comprehensive overview of the subject (slides are available), more detailed discussions were held in the plenary as well as in the breakout groups format. The following topics were discussed.

1. **Principle of distinction between combatants and civilians.** The main consequences of the distinction were underlined: 1) Combatant immunity — if falling into the hands of the other party to the conflict, combatants may not be prosecuted for taking part in hostilities, except war crimes, etc.; 2) Combatants are entitled to a prisoner-of-war (POW) status, but not in the case when they fail to distinguish themselves from the civilians; 3) Combatants enjoy no general protection from attack (except when *hors de combat*).

Participants agreed that there is limited clarity in the cyber context regarding several aspects. If there is doubt, the individual must be considered as a civilian. It was also asked that if a code qualifies a weapon, how to carry them openly (traditionally, one minimum requirement for combatant status is that they carry weapons openly during military operations). It was cautioned that if we decide in the cyber domain that international law could be interpreted in a more relaxed manner, then the adversary may relax also in other fields of IHL. In other words, if we believe in rule of law, we must apply IHL in cyber even if it is inconvenient as otherwise we would lose our right to complain if the adversary also applies more flexible interpretations.

2. **Civilian participation in hostilities in general** is a worrisome trend, partly resulting from the digitalization of societies. It was shared that there is a lower threshold for participation (everyone with a smartphone) and it is easy to do remotely. There is the ability to scale up (involving large groups in short periods of time); attack surface has extended immensely (we are all targets). E.g. civilians can upload the location of the enemy to an application for military needs (tactical intelligence); civilians can be at home hosting a DDoS attack from their computer, allowing others to use it for military purposes; or actively engaging in cyber operations themselves.

It was underlined that there needs to be more awareness among civilians when taking part in such activities, and what may be the risks. Some cautioned that if states encourage such forms of civilian engagement this would be a humanitarian problem and a potential protection gap; states have the passive precautions obligations — obligations to put in place effective measures to protect the civilian population against the dangers resulting from military operations. One participants pointed out that from a non-legal perspective, several private entities could be seen as “enablers”, and we should ask how to deal with those entities. It was shared that in some countries it may be illegal for civilians to participate in hostilities as only military personnel can do it.

3. **Direct participation in hostilities (DPH).** Three elements must be taken into account: 1) Threshold of harm (the act must adversely affect the military operation of the enemy); 2) Direct causation (there needs to be a direct causal link with the harm likely to result, e.g. information to be provided to be directly used for attack); 3) there must be a belligerent nexus (the act must be in support of a party to the conflict and to the detriment of another). There was no agreement over whether the intent of the individual matters (e.g. when the civilian does not know what will be the final impact of his/her activities). Participants also debated the individual self defence exception: if the company engages in the activities to defend its own networks, can they be seen as acting in individual self defence?

It was discussed which activities of the companies would qualify their personnel as DPH? Some participants concluded that providing defensive capabilities and intelligence operations would not reach the threshold of harm. It was also raised whether it matters for the legal assessment if the company is providing the service voluntarily? According to some, if you are actively feeding tactical data to cause harm, you can be considered a DPH. One participants pointed out that contractual obligation would also indicate DPH because there is commitment and knowledge about your services being used to cause harm; another disagreed and said that simple provision of weapons is not enough to constitute DPH.

There was also a discussion on if an individual is involved in DPH, e.g. running a malware from his computer, which results in direct harm to the adversary's military operations, then when can this individual be targeted (theoretically only during the attack) – when he is sitting at his computer; or during the time period the malware is running (but he might be away from the computer, e.g. at the supermarket).

There was also a discussion on the exact meaning of the “direct link” and “chain of causation” between the activity of the civilian and the military damage.

4. **Dual use technologies.** There was a question on how to qualify the members of companies that provide both civilian and military services. In the context of the scenarios, there were some opinions that the employees of the company Moonshade, which provided Woodland with high-bandwidth internet access via satellite connection, would not qualify as DPH just by providing services to the military, and suggestions that there was too remote causality and not enough nexus. Others suggested that there is a direct link between use of satellites and targeting.

Two principle questions emerged: 1) should there be a distinction between the employees that operate the military services under the company and the company itself? 2) if DPH is established, what can be legitimately targeted: the headquarters, satellites, infrastructure, anyone of the personnel (CEO, accountant, technicians, etc.) or something else? In terms of the first question there was an opinion by some that it would be more relevant to speak about the company, rather than the employees. The territorial aspects come into play – if the HQ would be targetable, would they blow up their HQ in another country? It was also asked whether the software of the services could be targeted.

5. **Uniforms and cyber operations.** There was a discussion about the requirement to distinguish combatants from civilians in cyberspace. Some participants suggested that since countries generally try to (also successfully) hide their identity anyway, the distinction between civilians and combatants is not relevant and ineffective in practice. One participant noted that today this principle means that we do not have to wear uniforms, but that the operations must be carried out by military personnel. Others thought that it was relevant to distinguish combatants at the moment of the attack; even more relevant if conducting the cyber operations from the enemy-controlled territory as the chances to get caught are higher. It was underlined that in practice cyber command personnel may not be wearing the uniform because they are not specifically “military”, e.g. not trained as such. E.g. when carrying out intelligence activities by intelligence personnel, uniforms are not needed in some countries as a way of drawing the line between military and civilian operations. Other participants voiced their opinion that if we believe in IHL, wearing uniforms (or any other distinction) is still relevant because otherwise there is a possibility to derogate from the principle of distinction; and it should be our goal to ensure that adversary activities amounting to hostilities are done by military personnel only. A parallel was drawn with the drone pilots, which in some countries need to wear uniforms when carrying out activities remotely.
6. **Harm.** Different cyber operations and the harm to military operations was discussed. It was generally agreed that information operations such as defacing websites would not negatively affect the military competence and capacity, even if causing mass panic. There were different opinions regarding the ransomware example and its effects on military operations – some thought that the threshold harm may be reached, others disagreed (too remote causal link between collecting the information and the actual harm). Some noted that the hackers' activities, which included sharing information about potential targets and hindering CI, may reach the threshold of harm. There was also a discussion of whether causing “harm” could also be viewed as an action of stopping an adversary from doing something, e.g. a civilian

scanning the network for vulnerabilities, identifying a malware that was aimed at fulfilling a military objective and deleting the malware (thereby hindering the adversary in carrying out its planned activities). Another example was shared: hacking the accounts of officials and giving orders, or deepfaking orders, resulting in negative effects on military operations. Equally, there was a debate of whether to assess each incident separately or take the collective impact into consideration. Several participants agreed that it is challenging to clearly identify the level of harm needed, and that drawing a clear line for that harm may even be unadvisable as adversaries may take advantage of that and operate just below it.

7. **Levée en masse.** When discussing the scenarios, there was generally an understanding that *levée en masse* does not apply to “ProLiberty”, since there was no clear territorial distinction and the timing was too late, because the conflict started in 2017. It was noted that there was some inner coordination between the hacktivist groups, but not with the government – so that the element of being “spontaneous” may have been fulfilled. This raised the issue of whether the hackers must need to know that they are in fact being coordinated by the government – e.g. looking at the instructions online, not knowing where these came from. It was pointed out that the hackers would want to argue that they were not coordinated by the government, in order to retain the POW status. Some participants noted that *levée en masse* was not a practical category when it came to cyber operations. The territorial element of *levée en masse* was discussed in greater detail, with various opinions on what must be the physical location of the participants of the *levée en masse* and whether it matters as much as the location of the effects of their activities.
8. **Prisoner of War status.** When it comes to the POW status applying to the hacktivists in the scenario, the majority of participants were of the opinion that the POW status does not apply, because the activity looked spontaneous, and not coordinated. If the hacktivist group would be modelled into a traditional loose chain of command, in some cases the POW status could apply. However, there were some opinions that the POW status would apply only if the group was under regular armed forces, or *levée en masse*.
9. **Extraterritoriality** is challenging, because it may bring up the issue of neutrality. It was cautioned that if the company is in another country and we do not target it because of its physical location, this may create a dangerous precedent. Another concern is that the civilians could geographically be anywhere and participate, and in that case other frameworks of IL may come to play. It was generally concluded that the extraterritorial application of IHL remained unsettled. Also, it was underlined that there are possible scenarios where a third country may become part of the conflict. Others were concerned about situations when a civilian of a third country decides to provide support to a party in conflict.
10. **Espionage.** Participants shared that the combatants who carry out espionage and are captured during its activities, would not get POW status. It is questionable what is the “location” of the individual carrying out espionage activities in the enemy networks – on its own territory or the enemy territory? It was suggested that if the spy manages to get back to their own territory they have re-gained POW status.

