联合国 A/76/136*

大 会

Distr.: General
13 July 2021
Chinese
Original: Arabic/Chinese/English/
French/Russian/Spanish

第七十六届会议

暂定项目表** 项目 96

从国际安全角度看信息和电信领域的发展

大会第 73/266 号决议所设从国际安全角度促进网络空间负责任国家行为政府专家组参与政府专家提交的关于各国使用信息和通信技术时国际法的适用主题的国家自愿贡献正式汇编

目录

* 由于技术原因于 2021 年 8 月 10 日重发。

** A/76/50。

21-09670 * (C) 110821 110821

一. 导言

1. 大会于 2018 年 12 月 22 日通过第 73/266 号决议，其中请秘书长在将于 2019 年基于公平区域分配成立的政府专家组的协助下，从以往政府专家组报告所载评估意见和建议出发，继续开展研究，以增进共同认识，有效执行应对国际信息安全领域现有和潜在威胁的可能合作措施，包括国家负责任行为的准则、规则和原则、建立信任措施和能力建设以及各国使用信息和通信技术时国际法的适用，并向大会第七十六届会议提交一份关于研究结果的报告，包括一份载有关于各国使用信息和通信技术时国际法的适用主题的参与政府专家国家贡献的附件。

2. 上述决议所设政府专家组于 2021 年 5 月 28 日以协商一致方式通过了报告。专家组报告(A/76/135)第 73 段指出，根据专家组的任务，将在裁军事务厅网站上发布参与政府专家关于各国使用信通技术时国际法的适用主题的国家自愿贡献的正式汇编。

3. 上文第 2 段提及的国家自愿贡献由各国的参与政府专家提交，载于本文件第二节。自愿贡献仅以提交语文发布。

二. 参与政府专家关于各国使用信通技术时如何适用国际法主题的自愿国家贡献

Australia

[Original: English]

Australia welcomes the opportunity to submit its national contribution on the subject of how international law applies to the use of information and communications technologies (ICT) by States as an annex to the report of the UN Group of Governmental Experts, as requested by the UN General Assembly in Resolution 73/266 (2019).

The international community recognises that existing international law – and in particular the UN Charter in its entirety – is applicable to State conduct in cyberspace and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. This is reflected in the 2013 and 2015 reports of the UN Group of Governmental Experts on Cyber (UN GGE) and the 2021 report of the UN Open Ended Working Group on Cyber (UN OEWG). The 2021 OEWG Report called upon States to avoid and refrain from taking any measures not in accordance with international law, and in particular the Charter of the United Nations, and concluded that further common understandings need to be developed on how international law applies to State use of ICTs.

A key part of the mandate of the GGE – including through these annexed national contributions – is to continue to study how international law applies to the use of ICTs by States. This question is a subject of ongoing consideration by States individually and collectively through the UN and other multilateral forums. Deepening our understanding of how international law applies is an iterative process, involving States forming national views and exchanging positions. Through internal consideration and international exchanges, States are building a deeper, clearer and more practical understanding of how international law applies to State behaviour in

cyberspace. Even where views differ, developing understandings of respective States' positions may increase predictability and reduce the risk of miscalculation, which can lead to escalation in State conduct. The contributions of States represented through experts as part of this GGE are an important part of this process and will be a valuable resource for the international community on key questions of how international law applies in cyberspace.

In 2020, Australia also submitted a non-paper to the UN OEWG on Cyber containing a series of case studies on the application of international law in cyberspace.

The case studies seek to demonstrate that existing treaties and customary international law provide a comprehensive and robust framework to address the threats posed by state-generated or sponsored malicious cyber activity. In particular, international law provides victim States with a 'tool kit' to identify breaches of international legal obligations, attribute those acts to the responsible State, seek peaceful resolution of disputes and, where the victim State deems appropriate, take lawful measures in response. In this way, the application of existing international law to cyberspace can enhance international peace and security by increasing the predictability of State behaviour, reducing the possibility of conflict, minimising escalation and preventing misattribution. The case studies are **annexed** to this submission and should be read in conjunction with it.

It is important to recognise that international law is most effective when States implement and adhere to their international legal obligations and, where necessary, cooperate to uphold international law and ensure accountability for violations.

In the cyber context, international law is one element in the 'framework for responsible State behaviour in cyberspace'. The other elements are: voluntary, non-binding norms ('norms'); confidence building measures; and capacity building. The 2015 GGE elaborated 11 norms, which were endorsed by consensus in UN General Assembly Resolution 70/237 (2015), as well as in the report of the 2021 OEWG which was itself endorsed by consensus in UN General Assembly Decision 75/816. The norms reflect the expectations and standards of the international community regarding responsible State behaviour in cyberspace, but they do not replace or alter States' binding obligations or rights under international law. Accordingly, the norms provide specific guidance, additional to international law, on what constitutes responsible State behaviour in the use of ICTs. This understanding of the relationship between international law and norms was affirmed by the OEWG in its 2021 report.

1. The United Nations Charter, the law on the use of force (*jus ad bellum*) and the principle of non-intervention

The United Nations Charter (UN Charter) and associated rules of customary international law apply to activities conducted in cyberspace. Article 2(3) of the UN Charter requires States to seek the peaceful settlement of disputes and Article 2(4) prohibits the threat or use of force by a State against the territorial integrity or political independence of another State, or in any manner inconsistent with the purposes of the UN. These obligations—and the UN Charter in its entirety—apply in cyberspace as they do in the physical realm.

The obligation to seek peaceful settlement of disputes does not impinge upon a State's inherent right to act in individual or collective self-defence in response to an armed attack. This right applies equally in the cyber domain as it does in the physical realm.

The UN Charter (Article 33) applies to international disputes involving cyber activities, the continuance of which are likely to endanger the maintenance of

international peace and security. States are required to seek the settlement of such disputes by peaceful means such as negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, and resort to regional agencies or arrangements, or other peaceful means of their own choice.

Resolution of a cyber dispute consistent with Chapter VI of the UN Charter (Pacific Settlement of Disputes) could include the parties referring the matter to the International Court of Justice. This would require that the necessary preconditions be met, including that the matter is admissible and that the Court has jurisdiction to hear it.

The UN Security Council may exercise its powers and responsibilities under Chapter VI and Chapter VII (Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression) of the UN Charter with respect to cyber activities endangering international peace and security.

In determining whether a cyber activity constitutes a use of force, States should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law. This involves a consideration of the intended or reasonably expected direct and indirect consequences of the cyber activity, including for example whether the activity could reasonably be expected to cause serious or extensive ('scale') damage or destruction ('effects') in the form of injury or death to persons, or damage or destruction (including to their functioning) to objects or critical infrastructure.

Harmful conduct in cyberspace that does not constitute a use of force may constitute a breach of the duty not to intervene in the internal or external affairs of another State. This obligation is encapsulated in Article 2(7) of the Charter and in customary international law.

A prohibited intervention is one that interferes by coercive means, either directly or indirectly, in matters that a State is permitted by the principle of State sovereignty to decide freely. Such matters include a State's economic, political, social and cultural systems and foreign policy. Coercive means are those that effectively deprive or are intended to deprive the State of the ability to control, decide upon or govern matters of an inherently sovereign nature.

The use by a State of cyber activities to prevent another State from holding an election, or manipulate the electoral system to alter the results of an election in another State, intervene in the fundamental operation of Parliament, or significantly disrupt the functioning of a States' financial systems would constitute a violation of the principle of non-intervention.

A use of force will be lawful when the territorial State consents, when it is authorised by the Security Council under Chapter VII of the UN Charter, or when it is taken pursuant to a State's inherent right of individual or collective self-defence in response to an armed attack, as recognised in Article 51 of the Charter.

Australia considers that the thresholds and limitations governing the exercise of self-defence under Article 51 apply in respect of cyber activities that constitute an armed attack and in respect of acts of self-defence that are carried out by cyber means. Thus, if a cyber activity—alone or in combination with a physical operation—results in, or presents an imminent threat of, damage equivalent to a traditional armed attack, then the inherent right to self-defence is engaged. Any use of force in self-defence must be necessary for the State to defend itself against the actual or imminent armed attack, and be a proportionate response in scope, scale and duration. Any reliance on Article 51 must be reported directly to the UN Security Council.

The rapidity of cyber activities, as well as their potentially concealed and/or indiscriminate character, raises new challenges for the application of established

principles. These challenges have been noted by Australia in explaining its position on imminence and the right of self-defence in the context of national security threats that have evolved as a result of technological advances. For example, in a speech to the University of Queensland in 2017, then Attorney-General, Senator the Hon. George Brandis QC, explained that:

> '[A] state may act in anticipatory self-defence against an armed attack when the attacker is clearly committed to launching an armed attack, in circumstances where the victim will lose its last opportunity to effectively defend itself unless it acts. This standard reflects the nature of contemporary threats, as well as the means of attack that hostile parties might deploy. Consider, for example, a threatened armed attack in the form of an offensive cyber operation, …which could cause large-scale loss of human life and damage to critical infrastructure. Such an attack might be launched in a split-second. Is it seriously to be suggested that a state has no right to take action before that split-second?'

2. International humanitarian law (*jus in bello*) and international human rights law

International humanitarian law (IHL) (including the principles of humanity, necessity, proportionality and distinction) applies to cyber activities within an armed conflict.

Australia considers that a cyber activity may constitute an 'attack' against an adversary under IHL if it rises to the same threshold as that of a kinetic 'attack' (or act of violence). The rules governing such attacks during armed conflict will apply to those kinds of cyber activities. Accordingly, it will be necessary to assess whether the cyber activity is sufficiently connected to hostilities and results in the reasonably foreseeable death or injury to individuals or damage and destruction to objects. IHL also provides rules that apply to cyber activities in an armed conflict that do not constitute or rise to the level of an 'attack', including the general protections afforded to the civilian population and individual civilians against dangers arising from military operations.

In accordance with the IHL principle of military necessity, a combatant is justified in using measures, not forbidden by international law, which are indispensable for securing complete submission of an enemy at the soonest moment. The principle cannot be used to justify actions prohibited by law, as the means to achieve victory are not unlimited.

The IHL principle of distinction seeks to ensure that only legitimate military objectives are attacked. Distinction has two components. The first, relating to personnel, seeks to maintain the distinction between combatants (who may be attacked), and civilians or non-combatants (including protected persons). The second component distinguishes between objects which are targetable as legitimate military objectives, and civilian and protected objects.

The IHL principle of proportionality prohibits the launching of an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

Australia, and other States parties to Additional Protocol I to the Geneva Conventions of 1949 are required under Article 36 to determine whether the employment of new weapons, or means or method of warfare, would, in some or all circumstances be prohibited by Additional Protocol I or any other rule of international law applicable to that State. A cyber capability could, in certain circumstances, constitute a 'weapon, or a means or method of warfare' within the meaning of Article 36 and require a review in accordance with Article 36 obligations.

In armed conflict, Australian military capabilities are employed within a well-established system of command and control, within applicable legal frameworks, and subject to orders, directives and procedures. This includes approved targeting procedures. Cyber activities are no different. Where cyber actions or activities amount to an attack under IHL, as for conventional activities, Australian targeting procedures comply with the requirements of IHL. Trained legal officers are available to support Commanders with advice to ensure that Australia satisfies its obligations under international law and operates in accordance with its domestic legal requirements.

International human rights law (IHRL) also applies to State conduct in cyberspace. Under IHRL, States have obligations to protect relevant human rights of individuals under their jurisdiction, including the right to privacy, where those rights are exercised or realised through or in cyberspace. Subject to lawful derogations and limitations, States must ensure without distinction individuals' rights to privacy, freedom of expression and freedom of association online.

3. General principles of international law, including the law on State responsibility

The customary international law on State responsibility, much of which is reflected in the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA), applies to State behaviour in cyberspace. Under the law on State responsibility, there will be an internationally wrongful act of a State when its conduct in cyberspace – whether by act or omission – is attributable to it and constitutes a breach of one of its international obligations.

To the extent that a State enjoys the right to exercise sovereignty over objects and activities within its territory, it necessarily shoulders corresponding responsibilities to ensure those objects and activities are not used to harm other States. In this context, we note it may not be reasonable to expect (or even possible for) a State to prevent all malicious use of ICT infrastructure located within its territory. However, in Australia's view, if a State is aware of an internationally wrongful act originating from or routed through its territory, and it has the ability to put an end to the harmful activity, that State should take reasonable steps to do so consistent with international law.

States are entitled, in their sole discretion, and based on their own judgement, to attribute unlawful cyber activities to another State. States should act reasonably when drawing conclusions based on the facts before them.

A cyber activity will be attributable to a State under international law where, for example, the activity was conducted by an organ of the State; by persons or entities exercising elements of governmental authority; or by non-State actors operating under the direction or control of the State.

Australia recognises the need to distinguish between different attribution assessments, including factual attribution (which includes an assessment of technical and other contextual information) and legal attribution (that there has been a breach of international law), as well as the political decision to convey – publicly or privately – those attribution assessments.

If a State is a victim of malicious cyber activity, which is attributable to a perpetrator State, the victim-State may be able to take countermeasures under certain circumstances. Countermeasures are measures, which would otherwise be unlawful, taken to secure cessation of, or reparation for, the other State's unlawful conduct. Countermeasures may be cyber in nature or taken through alternative means, such as temporarily not performing certain bilateral treaty obligations owed to a State.

Countermeasures in cyberspace cannot amount to a use of force and must be proportionate.

States are able to respond to other States' malicious activity with acts of retorsion, which are unfriendly acts that are not inconsistent with any of the State's international obligations.

If a State is the victim of harmful conduct in cyberspace, that State could be entitled to remedies in the form of restitution, compensation or satisfaction. In the cyber context, this may mean that the victim-State could, for example, seek replacement of damaged hardware or compensation for the foreseeable physical and financial losses resulting from the damage to servers, as well as assurances or guarantees of non-repetition.

28 May 2021
[Annex: cyber case studies]

Annex

Australia Non Paper
Case studies on the application of international law in cyberspace

The international community recognises that existing international law – and in particular the UN Charter in its entirety – is applicable to state conduct in cyberspace and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. This is reflected in the 2013 and 2015 reports of the UN Group of Governmental Experts on the use of Information Communications Technologies in the Context of International Security (UNGGE),[1] as adopted by the UN General Assembly.[2] Australia's position on how international law governs state conduct in cyberspace is presented in the International Cyber Engagement Strategy (2017), Annex A,[3] as supplemented by the 2019 International Law Supplement.[4]

These case studies apply international law to standalone hypothetical scenarios, demonstrating that existing treaties and customary international law provide a comprehensive and robust framework to address the threats posed by state-generated or sponsored malicious cyber activity. In particular, international law provides victim states with a "tool kit" to identify breaches of international legal obligations, attribute those acts to the responsible state, seek peaceful resolution of disputes and, where the victim state deems appropriate, take lawful measures in response. The case studies illustrate that the application of existing international law to cyberspace can enhance international peace and security by increasing predictability of state behaviour, reducing the possibility of conflict, minimising escalation and preventing misattribution.

The case studies represent fictional scenarios and are not based on actual actors or events. They are intended to illustrate potential options rather than recommend a course of action. They do not purport to represent how Australia could or would respond to any malicious cyber activity directed against it, or purport to provide a comprehensive view on potential response options or the international law issues raised in any specific scenario.

Scenario 1 – Cyber operations by State B on government systems and websites of State A

State A undertakes major reforms to its domestic company law and tax code that are consistent with its international obligations. In order to implement the new laws – including to allow State A's tax office and corporate regulator to monitor and enforce new requirements on companies – State A requires all registered companies to disclose certain information via a government website. State B opposes the reforms because it considers they unfairly impact on the interests of companies from State B

[1] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013) UN Doc A/68/98 para 19; Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) UN Doc A/70/174 para. 24.

[2] UNGA Resolution 68/243 (9 January 2014) UN Doc A/RES/68/243; UNGA Resolution 70/237 (30 December 2015) UN Doc A/RES/70/237.

[3] Available at https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/annexes.html#Annex-A and also enclosed at **Attachment 1**.

[4] Available at https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/2019_international_law_supplement.html and also enclosed at **Attachment 2**.

operating in State A. In an attempt to prevent State A from implementing the reforms, State B, through its Department of Defence, conducts a series of cyber operations that prevent use of the website and disable government systems of State A's tax office and corporate regulator. As a result, State A is incapable of regulating companies' compliance with the new laws for a substantial period and has no choice but to indefinitely postpone implementation of the new tax reforms. State A also loses significant tax revenue.

International law may assist State A in the following ways:

First, it provides **rules of legal attribution** – contained in the customary international law on state responsibility, much of which is reflected in the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts – meaning that acts of the Department of Defence, as an organ of State B, would be attributable to State B.

Second, it **defines states' rights and obligations**, including the international law duty not to intervene in the internal affairs of another state (prohibited intervention). State B's conduct could constitute a prohibited intervention on the basis that it was a coercive interference in matters which State A is entitled as a matter of state sovereignty to decide freely, including its economic system. However, establishing the aforementioned elements of prohibited intervention would depend on the circumstances, including the extent of economic damage and the loss of government control over economic policy.

Third, if State B's conduct violated international law, it would entitle State A to **invoke the international legal responsibility** of State B, and State A could demand that State B cease the unlawful act/s (if they were continuing) and make full reparation for State A's injuries. Reparation could include restoring full access to relevant websites and providing compensation for any financially assessable damage. As international law governs the dispute, State A may seek to pursue resolution through legal as well as political avenues including, for example, by seeking a resolution consistent with the Charter of the United Nations, including Chapter VI (*Pacific Settlement of Disputes*)[5], which could include referring the dispute to the International Court of Justice (ICJ) where the necessary preconditions had been met (including admissibility and jurisdiction).

Fourth, if State B's conduct violated international law, it would entitle State A to take **countermeasures** – acts which would ordinarily be unlawful – in response to State B's wrongdoing. Countermeasures could be cyber in nature or taken through alternative means – such as temporarily not performing certain bilateral treaty obligations owed to State B. However, State A would need to ensure that such countermeasures:

- were directed against State B;
- *did not* constitute a threat or use of force, violate fundamental human rights, humanitarian obligations prohibiting reprisals, or peremptory international legal norms;

[5] For example: Article 33(1) of the UN Charter provides that "The parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice." In *Security Our Common Future: An Agenda for Disarmament* (Office for Disarmament Affairs, 2018) the UN Secretary-General commits to "make available his good offices to contribute to the prevention and peaceful settlement of conflict stemming from malicious activity in cyberspace".

- were reversible (as far as possible);
- were proportionate to the injury suffered by State A; and
- were intended to induce State B to comply with its international legal obligations.

International law would not preclude State A from taking **acts of retorsion**, which are unfriendly acts that are not inconsistent with the international obligations of State A, including, for example, declaring diplomats from State B in State A *persona non grata*.

Scenario 2 – State A's territory/infrastructure used by State B to conduct malicious cyber activities against State C

State B's Department of Defence conducts malicious cyber activities against State C that are routed through servers located on State A's territory, without its knowledge. The malicious cyber activities conducted by State B are contrary to the rights of State C (although they do not constitute an unlawful use of force). State A's relationship with State C could be damaged.

International law may assist State A in the following ways:

First, it provides **rules of legal attribution**, under which the unlawful acts of State B could not be attributed to State A. The rules of attribution (as outlined in Scenario 1) provide a clear legal framework for connecting the conduct of an individual or an entity to a state; this connection would not be established in the present case between State B's Department of Defence and State A. Rather, the acts of the Department of Defence would be attributable to State B as an organ of that state exercising executive functions. Attribution would also be made out against State B if it used a proxy acting on its instructions, or under its direction or control, to carry out the relevant acts. Additionally, State A would not be considered responsible for aiding and assisting State B because its lack of knowledge of the wrongful acts and its lack of intent to aid or assist the wrongful acts would mean that it could not have been complicit in the commission of those acts. Therefore, State C could not make a legal attribution of the wrongful conduct to State A.

Second, as a result, State A **could not be considered directly responsible for any unlawful act** committed by State B against State C. Accordingly, State C could not pursue dispute resolution through legal avenues (including the ICJ, as outlined in Scenario 1) against State A in relation to State B's wrongdoing; although it could do so against State B. Additionally, assuming State A could not have been aware of the activity taking place from its territory, it did not act contrary to the norm of responsible state behaviour in cyberspace to not knowingly allow its territory to be used for internationally wrongful acts using ICTs,[6] or in violation of any applicable international obligations.

Third, as State A is not directly responsible for any unlawful act committed by State B against State C, State C could not take any **countermeasures** – acts that would ordinarily be unlawful – against State A in response to State B's conduct. Were it to do so, State A would itself be entitled to respond through countermeasures and seek remedies.

Note: this scenario details how international law would assist State A (whose territory/infrastructure was used without its knowledge by State B to conduct

[6] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) UN Doc A/70/174 para. 13(c) [see, also, para. 13(h)].

malicious activity against State C). Separately, and provided all requirements were met (see Scenario 1), State C could invoke the international legal responsibility of State B and pursue a legal and/or political resolution and take countermeasures and/or acts of retorsion against it.

Scenario 3 – State B conducts a major offensive cyber operation that constitutes a serious threat to State A's national security

Amid growing tensions between State A and State B,[7] the armed forces of State B conduct a major offensive cyber operation against State A, destroying servers located in State A used by State A's military headquarters. This renders State A unable to communicate with naval vessels operating in international waters off the coast of State B. It will take several months to replace the destroyed servers, at substantial cost.

International law may assist State A in the following ways:

First, it provides **rules of legal attribution**, meaning that under the customary international law on state responsibility (as outlined in Scenario 1), the acts of the armed forces, as an organ of State B, would be attributable to State B.

Second, it **defines states' rights and obligations**, meaning that State B's cyber operation may constitute an unlawful use of force contrary to Article 2(4) of the UN Charter against State A (unless such actions were taken in self-defence or authorised under a Chapter VII resolution of the UN Security Council). This would turn on whether the operation caused damage to State A's infrastructure and objects (its military servers) and subsequent impact on the functioning of its military communications systems that was akin in scale and effects to a traditional kinetic operation that would rise to the level of a use of force.

Third, assuming State B's conduct violated international law, it would entitle State A to **invoke the international legal responsibility** of State B and demand that State B cease unlawful act/s (if they were continuing) and make full reparation for State A's injuries. Reparation could entail compensation for financially assessable damage, as well as assurances or guarantees of non-repetition. As international law governs the dispute, State A may seek to pursue resolution through legal as well as political avenues including, for example, by seeking a resolution consistent with the Charter of the United Nations, including Chapter VI (*Pacific Settlement of Disputes*)[8] (which could include the International Court of Justice, as outlined in Scenario 1) and/or Chapter VII (*Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression*).[9]

Fourth, if State B's conduct violated international law, it would entitle State A to take **countermeasures** – acts which would ordinarily be unlawful – in response to State B's wrongdoing. Countermeasures could be cyber in nature or taken through alternative means – such as implementing otherwise unlawful tariffs on trade in important goods/services from State B. However, State A would need to ensure that such countermeasures:

[7] For the purposes of this scenario, there is not a state of armed conflict between State A and State B immediately prior to State B's offensive cyber operation.

[8] See note 5 above.

[9] For example: Article 39 of the UN Charter provides that "The [UN] **Security Council** shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42 to maintain or restore international peace and security."

- were directed against State B;
- did not constitute a threat or use of force, violate fundamental human rights, humanitarian obligations prohibiting reprisals, or peremptory international legal norms;
- were reversible (as far as possible);
- were proportionate to the injury suffered by State A; and
- were intended to induce State B to comply with its international legal obligations.

Fifth, if the cyber operation constituted an "armed attack", as recognised under Article 51 of the UN Charter, State A would be entitled to use force pursuant to its inherent right of **self-defence** against State B. The use of force in self-defence may be cyber in nature or conducted through kinetic means. However, the right to self-defence would require that State A only use force where it is necessary to repel the actual or imminent armed attack and that such force be a proportionate response in scope, scale and duration. The measures taken by State A would need to be immediately reported to the UN Security Council.

International law would not preclude State A from taking **acts of retorsion**, which are unfriendly acts that are not inconsistent with the international obligations of State A, including, for example, declaring diplomats from State B in State A *persona non grata*.

ATTACHMENT 1

2017 - AUSTRALIA'S POSITION ON THE APPLICATION OF INTERNATIONAL LAW TO STATE CONDUCT IN CYBERSPACE

Existing international law provides the framework for state behaviour in cyberspace. This includes, where applicable, the law regarding the use of force, international humanitarian law (IHL), international human rights law, and international law regarding state responsibility.

In this respect, Australia notes that the centrality of international law and its application to states' use of cyberspace was affirmed in 2013 in the consensus report of the third *United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, which was chaired by Australia, and reaffirmed in the 2015 report of the UNGGE.

However, Australia recognises that activities conducted in cyberspace raise new challenges for the application of international law, including issues of sovereignty, attribution and jurisdiction, given that different actors engage in a range of cyber activities which may cross multiple national borders. This annex sets out Australia's views on these issues.

1. The United Nations Charter and the law on the use of force (*jus ad bellum*) apply to activities conducted in cyberspace.

The Charter of the United Nations requires states to seek peaceful settlements of disputes. This obligation extends to cyberspace and requires states to resolve cyber incidents peacefully without escalation or resort to the threat or use of force. This requirement does not impinge upon a state's inherent right to act in individual or collective self-defence in response to an armed attack, which applies equally in the cyber domain as it does in the physical realm.

In determining whether a cyber attack, or any other cyber activity, constitutes a use of force, states should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law. This involves a consideration of the intended or reasonably expected direct and indirect consequences of the cyber attack, including for example whether the cyber activity could reasonably be expected to cause serious or extensive ('scale') damage or destruction ('effects') to life, or injury or death to persons, or result in damage to the victim state's objects, critical infrastructure and/or functioning.

2. For cyber operations constituting or occurring within the context of an international or non-international armed conflict, the relevant international humanitarian law (*jus in bello*) will apply to the conduct of these cyber activities.

International humanitarian law (IHL) (including the principles of humanity, necessity, proportionality and distinction) applies to cyber operations within an armed conflict.

The IHL principle of proportionality prohibits the launching of an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

The IHL principle of military necessity states that a combatant is justified in using those measures, not forbidden by international law, which are indispensable for securing complete submission of an enemy at the soonest moment. The principle cannot be used to justify actions prohibited by law, as the means to achieve victory are not unlimited.

The IHL principle of distinction seeks to ensure that only legitimate military objects are attacked. Distinction has two components. The first, relating to personnel, seeks to maintain the distinction between combatants and non-combatants or military and civilian personnel. The second component distinguishes between legitimate military targets and civilian objects.

All Australian military capabilities are employed in line with approved targeting procedures. Cyber operations are no different. Australian targeting procedures comply with the requirements of IHL and trained legal officers provide decision-makers with advice to ensure that Australia satisfies its obligations under international law and its domestic legal requirements.

For example, Australia considers that, if a cyber operation rises to the same threshold as that of a kinetic 'attack under IHL', the rules governing such attacks during armed conflict will apply to those kinds of cyber operations.

3. For cyber activities taking place outside of armed conflict, general principles of international law, including the law on state responsibility, apply.

It is a longstanding rule of international law that, if a state acts in violation of an international obligation, and that violation is attributable to the state, that state will be responsible for the violation.

The customary international law on state responsibility, much of which is reflected in the International Law Commission's *Articles on the Responsibility of States for Internationally Wrongful Acts*, apply to state behaviour in cyberspace.

To the extent that a state enjoys the right to exercise sovereignty over objects and activities within its territory, it necessarily shoulders corresponding responsibilities to ensure those objects and activities are not used to harm other states. In this context, we note it may not be reasonable to expect (or even possible for) a state to prevent all malicious use of ICT infrastructure located within its territory. However, in Australia's view, if a state is aware of an internationally wrongful act originating from or routed through its territory, and it has the ability to put an end to the harmful activity, that state should take reasonable steps to do so consistent with international law.

If a state is a victim of malicious cyber activity which is attributable to a perpetrator state, the victim state may be able to take countermeasures against the perpetrator state, under certain circumstances. However, countermeasures that amount to a use of force are not permissible. Any use of countermeasures involving cyberspace must be proportionate. It is acknowledged that this raises challenges in identifying and assessing direct and indirect effects of malicious cyber activity, in order to gauge a proportionate response. The purpose of countermeasures is to compel the other party to desist in the ongoing unlawful conduct.

ATTACHMENT 2

2019 - SUPPLEMENT TO AUSTRALIA'S POSITION ON THE APPLICATION OF INTERNATIONAL LAW TO STATE CONDUCT IN CYBERSPACE

In the *International Cyber Engagement Strategy* (2017) (Strategy), Australia committed to periodically publish its position on the application of relevant international law to state conduct in cyberspace. The first such publication appeared in Annex A to the Strategy. This document is the second publication and is aimed at further elaborating Australia's position on applicable international law as expressed in the Strategy. As such, it should be read as a supplement to that document.

Application and development of international law

The Strategy recognised the well-established position that existing international law - including the UN Charter in its entirety - provides the framework for responsible state behaviour in cyberspace. The international community, including the permanent members of the United Nations (UN) Security Council recognised this in the 2013 and 2015 reports of the UN Group of Governmental Experts on the use of Information Communications Technologies in the Context of International Security (UNGGE), as adopted by the UN General Assembly. Australia also acknowledged that activities conducted in cyberspace raise new challenges for how international law applies. To deepen understandings and set clear expectations, Australia encourages states to be transparent in how they interpret existing international law as it applies to state conduct in cyberspace. The Strategy, and this supplement, form part of Australia's ongoing effort to make its views on the applicability of international law public.

The law on the use of force (*jus ad bellum*) and the principle of non-intervention

The United Nations Charter (Charter) and associated rules of customary international law apply to activities conducted in cyberspace. Article 2(3) of the Charter requires states to seek the peaceful settlement of disputes and Article 2(4) prohibits the threat or use of force by a state against the territorial integrity or political independence of another state, or in any manner inconsistent with the purposes of the UN. In the Strategy, Australia made clear that these obligations – and the UN Charter in its entirety, including those obligations, apply in cyberspace as they do in the physical realm.

A use of force will be lawful when the territorial state consents, it is authorised by the Security Council under Chapter VII of the UN Charter or when it is taken pursuant to a state's inherent right of individual or collective self-defence in response to an armed attack, as recognised in Article 51 of the Charter. Australia considers that the thresholds and limitations governing the exercise of self-defence under Article 51 apply in respect of cyber operations that constitute an armed attack and in respect of acts of self- defence that are carried out by cyber means. Thus if a cyber operation – alone or in combination with a physical operation – results in, or presents an imminent threat of, damage equivalent to a traditional armed attack, then the inherent right to self-defence is engaged. The rapidity of cyber attacks, as well as their potentially concealed and/or indiscriminate character, raises new challenges for the application of established principles. These challenges have been raised by Australia in explaining its position on the concept of imminence and the right of self-defence in the context of national security threats that have evolved as a result of technological advances (see Figure 1).

FIGURE 1 – IMMINENCE AND CYBER OPERATIONS

> *"[A] state may act in anticipatory self-defence against an armed attack when the attacker is clearly committed to launching an armed attack, in circumstances where the victim will lose its last opportunity to effectively defend itself unless it acts.*
>
> *This standard reflects the nature of contemporary threats, as well as the means of attack that hostile parties might deploy.*
>
> *Consider, for example, a threatened armed attack in the form of an offensive cyber operation (and, of course, when I say 'armed attack', I mean that term in the strict sense of Article 51 of the Charter). The cyber operation could cause large-scale loss of human life and damage to critical infrastructure. Such an attack might be launched in a split-second. Is it seriously to be suggested that a state has no right to take action before that split-second?*"
>
> Attorney-General, Senator the Hon. George Brandis QC,
> University of Queensland, 11 April 2017

Harmful conduct in cyberspace that does not constitute a use of force may still constitute a breach of the duty not to intervene in the internal or external affairs of another state. This obligation is encapsulated in Article 2(7) of the Charter and in customary international law. A prohibited intervention is one that interferes by coercive means (in the sense that they effectively deprive another state of the ability to control, decide upon or govern matters of an inherently sovereign nature), either directly or indirectly, in matters that a state is permitted by the principle of state sovereignty to decide freely. Such matters include a state's economic, political, and social systems, and foreign policy. Accordingly, as former UK Attorney-General Jeremy Wright outlined in 2018, the use by a hostile State of cyber operations to manipulate the electoral system to alter the results of an election in another State, intervention in the fundamental operation of Parliament, or in the stability of States' financial systems would constitute a violation of the principle of non-intervention.

International humanitarian law (*jus in bello*) and international human rights law

The Strategy and the 2015 Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174), discussed the applicability of international humanitarian law (IHL) to cyber operations in armed conflict, including the principles of humanity, military necessity, proportionality and distinction. Australia considers that, if a cyber operation rises to the same threshold as that of a kinetic 'attack' (or act of violence) under IHL, the rules governing such attacks during armed conflict will apply to those kinds of cyber operations. Applicable IHL rules will also apply to cyber operations in an armed conflict that do not constitute or rise to the level of an 'attack', including the principle of military necessity and the general protections afforded to the civilian population and individual civilians with respect to military operations.

International human rights law (IHRL) also applies to the use of cyberspace (see e.g. Figure 2). States have obligations to protect relevant human rights of individuals under their jurisdiction, including the right to privacy, where those rights are exercised or realised through or in cyberspace. Subject to lawful derogations and limitations, states must ensure without distinction individuals' rights to privacy, freedom of expression and freedom of association online.

FIGURE 2 – COMMONWEALTH CYBER DECLARATION

"Recognising the potential for a free, open, inclusive and secure cyberspace to promote economic growth for all communities and to act as an enabler for realisation of the Sustainable Development Goals across the Commonwealth, we: …

5. Affirm that the same rights that citizens have offline must also be protected online."

Commonwealth Heads of Government Declaration
20 April 2018

General principles of international law, including the law on state responsibility

In the Strategy, Australia recognised that the law on state responsibility, much of which is reflected in the International Law Commission's Articles on the Responsibility of states for Internationally Wrongful Acts, applies to state behaviour in cyberspace. Under the law on state responsibility, there will be an internationally wrongful act of a state when its conduct in cyberspace – whether by act or omission – is attributable to it and constitutes a breach of one of its international obligations.

Australia will, in its sole discretion, and based on its own judgement, attribute unlawful cyber operations to another state. In making such decisions, Australia relies on the assessments of its law enforcement and intelligence agencies, and consultations with its international partners (see e.g. Figure 3). A cyber operation will be attributable to a state under international law where, for example, the operation was conducted by an organ of the state; by persons or entities exercising elements of governmental authority; or by non-state actors operating under the direction or control of the state.

As outlined in the Strategy, if a state is a victim of malicious cyber activity which is attributable to a perpetrator state, the victim state may be able to take countermeasures (whether in cyberspace or through another means) against the perpetrator state, under certain circumstances. Countermeasures are measures, which would otherwise be unlawful, taken to secure cessation of, or reparation for, the other state's unlawful conduct. Countermeasures in cyberspace cannot amount to a use of force and must be proportionate. States are able to respond to other States' malicious activity with acts of retorsion, which are unfriendly acts that are not inconsistent with any of the State's international obligations.

If a state is the victim of harmful conduct in cyberspace, that state could be entitled to remedies in the form of restitution, compensation or satisfaction. In the cyber context, this may mean that the victim-state could for example seek replacement of damaged hardware or compensation for the foreseeable physical and financial losses resulting from the damage to servers, as well as assurances or guarantees of non-repetition.

Brazil

[Original: English]

Brazil firmly believes that in their use of information and communications technologies, States must comply with international law, including the United Nations Charter, international human rights law and international humanitarian law. The United Nations and other regional organizations have recognized that international law, and in particular the Charter of the United Nations, is applicable to States' ICT-related activity in cyberspace and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.[10] Hence, in current discussions, the question is no longer whether, but how international law applies to the use of ICTs by States.

While analogies in relation to the physical world might work most of the time to determine the manner in which international law applies, cyberspace's unique characteristics create new situations that international law was not originally designed to address. The interconnectivity of information systems, the intangible components of cyberspace, the fluidity of jurisdictions and the potential anonymity of cyber operations, among other factors, pose new challenges to international law, whose development has been based on a physical and territorial international order.

The development and use of new technologies will inevitably raise questions both of *lex lata* and *lege ferenda.* Law will often be outpaced by scientific progress, which in turn tends to generate considerable uncertainty about the application of certain international rules.[11] Legal uncertainty, particularly in the realm of peace and security, can lead to unwarranted insecurity and increased risks of conflict.

To the extent that interpretations of how international law applies to the use of ICT by States diverge, the risk of unpredictable behavior, misunderstandings and escalation of tensions increases. Therefore, it is important to identify convergence amongst States on this matter and, where divergences are identified, to jointly work towards increased coherence in the interpretation of existing rules. If necessary, development of additional norms should also be considered as a means to fill potential legal gaps and resolve remaining uncertainties.

The current paper highlights Brazil's views on how international law applies to the use of ICTs by States. Given the broad scope of international law, only some aspects will be covered. In developing this assessment, Brazil has followed the traditional sources of international law, as enshrined in article 38 of the ICJ Statute. Academic works and expert reports, such as the Talinn Manual and the ICRC Position Paper, are considered as important reference material.

1. Sovereignty

State sovereignty is one of the founding principles of international law. As the ICJ has stated in the Corfu Channel Case, "between independent States, the respect

[10] United Nations Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 19, UN DOC. A/68/98 (June, 24, 2013); United Nations Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, paras.13 , 24 and 28(b) UN DOC A/70/174 (22 July 2015); United Nations Report of the Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security, para. 71(b) (May 2021, advance copy).

[11] Oliver Kessler and Wouter-Werner, "Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare," 26 *Leiden Journal of International Law* 793 (2013), pp. 802–807, p. 807.

for territorial sovereignty is an essential foundation for 'international relations'".[12] It is applicable as a standalone rule, including to the use of ICTs by States, and entails an independent obligation of "every State to respect the territorial sovereignty of others"[13]. Currently, there is neither broad state practice nor sufficient *opinio juris* to generate new customary international norm allowing for the violation of State sovereignty, including by means of ICTs.

Violations of State sovereignty by another State, including by means of ICTs, constitute an internationally wrongful act and entail the international responsibility of the State in violation. Interceptions of telecommunications, for instance, whether or not they are considered to have crossed the threshold of an intervention in the internal affairs of another State, would nevertheless be considered an internationally wrongful act because they violate state sovereignty[14]. Similarly, cyber operations against information systems located in another State's territory or causing extraterritorial effects might also constitute a breach of sovereignty.

2. Non-intervention

The principle of non-intervention, which is considered customary international law, refers to "the right of every sovereign State to conduct its affairs without outside interference".[15] In the Declaration on the Principles of International Law concerning Friendly Relations and Co-operation among States,[16] the General Assembly affirmed that "the strict observance by States of the obligation not to intervene in the affairs of any other State is an essential condition to ensure that nations live together in peace with one another". Even though Resolution 2625 (XXV) preceded the widespread use of ICTs, the customary norm prohibiting intervention in the internal affairs of another State applies irrespective of the means or medium used and extends to the use of ICTs by States.

To violate the principle of non-intervention, the malicious use of ICTs against another State must involve an element of coercion affecting the right of the victim State to freely choose its political, economic, social and cultural system, and to formulate its foreign policy.[17] If attributable to a State, this breach entails this State's international responsibility.

There has been a growing discussion on whether cyberoperations aimed at interfering in the electoral processes of another State could amount to violations of the principle of non-intervention. Considering that elections are at the core of a State's internal affairs, should the malicious use of ICTs against a State involve some level of coercion, then it must be prohibited by the principle of non-intervention.

3. Use of force

As stated in previous reports of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, international law is applicable to the use of ICTs by States. This includes the legal prohibition of the use of force in international

[12] Corfu Channel Case, ICJ, 1949, 35; See also Schwarzenberger, p 219.

[13] ICJ, Nicaragua, Merits, p. 111.

[14] A/67/946.

[15] ICJ, Nicaragua, Merits, pp 106-108.

[16] General Assembly Resolution 2625 (XXV).

[17] ICJ, Nicaragua, Merits, p 108.

relations, which is enshrined in the UN Charter[18] and is also part of customary international law. It is a peremptory norm,[19] to which only two exceptions are permitted: self-defense and authorization under Chapter VII of the Charter.

The United Nations Charter does not refer to specific weapons or other means of use of force, and therefore the legal prohibition applies to all of them[20]. Cyber operations may amount to an illegal use of force if they are attributable to a State and if their impact is similar to the impact of a kinetic attack. It is generally understood that, to date, no state has claimed that the rule prohibiting the use of force was violated due to the conduction of a cyberattack. The lack of such a precedent only reinforces the need for caution when making analogies between cyber and kinetic actions in assessments related to *jus ad bellum*.

General Assembly Resolution 3314(XXIX), which contains the definition of aggression, enumerates a series of acts that qualify as such: invasion of territory by armed forces, military occupation, bombardments or the use of any weapons against the territory of another state, blockade of the ports or coasts by the armed forces, among others. Although it is not binding, GA Res 3314(XXIX) has been considered highly authoritative and has guided the ICJ in its caselaw.[21] In many instances, it might prove difficult to establish a direct analogy between the acts listed in GA Res 3314 (XXIX) and cyber operations, due to their unique characteristics. Therefore, it is advisable to update the multilateral understanding of which acts amount to the use of force and aggression, so as to include instances of cyberattacks. While it might be challenging to find consensus on grey areas, such as the characterization of digital attacks with no direct physical effects, there are points of convergence that should be consolidated multilaterally to provide more clarity and legal certainty.

Amongst the gravest forms of the use of force in international relations are armed attacks,[22] which trigger the right of states to resort to self-defense, in accordance with article 51 of the UN Charter. Being self-defense an exception to the general principle on the prohibition to the use of force, it needs to be interpreted restrictively. This view is in line with the case law of the International Court of Justice, the principal judicial organ of the United Nations.[23]

As a consequence, self-defense is only triggered by an armed attack undertaken by or attributable to a State.[24] It is not possible to invoke self-defense as a response to acts by non-State actors, unless they are acting on behalf or under the effective control of a state. This norm becomes even more relevant with cyber operations, where technical, legal and operational challenges to determine attribution might make it impossible to verify potential abuses of the right of self-defense, which in turns creates the risk of low impact persistent unilateral military action undermining the collective system established under the Charter.

---

[18] Charter of the United Nations, art. 2(4).

[19] International Law Commission, Commentaries to the 1966 draft articles on the law of treaties.

[20] ICJ, Advisory Opinion on Nuclear Weapons, p. 244.

[21] ICJ, Armed Activities, p. 223.

[22] ICJ, Nicaragua, p. 91; ICJ, Oil Platforms (2003), para 64.

[23] See, e.g., ICJ, Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), p. 123 (“Article 51 of the Charter may justify a use of force in self-defence only within the strict confines there laid down").

[24] ICJ, Armed Activities, p. 223.

In the same vein, contemporary international law does not allow for self-defense on the basis that the territorial state would be "unwilling and unable" to repress non-state actors whose cyber acts have extraterritorial effects. The definition of "armed attack" is limited to the use of force attributable to a state and, therefore, actions from non-state actors with similar effects might amount to serious crimes, but not an "armed attack". If such a situation arises, the territorial state should adopt measures, in good faith and within its capabilities, to cease the action and ensure accountability. If it fails to do so, this omission might constitute an internationally wrongful act, thus entailing this states' international responsibility. According to customary international law, in this case the victim state is entitled to remedies, to be pursued only through peaceful means.

Moreover, self-defense should be a temporary remedy. Member states that exercise their right to self-defense must immediately report it to the Security Council, in line with article 51 of the Charter. Given the novelty of cyberattacks and the uncertainties related to it, reporting to the Security Council is even more important. As the ICJ highlighted, "the absence of a report may be one of the factors indicating whether the State in question was itself convinced that it was acting in self-defense".[25] Once the incident is reported to the Security Council, it is expected that the temporary act of self-help is replaced by collective action, adopted and pursued in line with the UN Charter.

For Brazil, the right to self-defense exists once there is an actual or imminent armed attack. Under international law, there is no right to "preventive self-defense" - a notion that does not find legal grounds neither in art. 51 of the Charter nor in customary international law. Finally, as with responses to armed activities using conventional weapons, self-defense against armed attacks caused by digital means must be necessary and proportionate.[26]

4. State Responsibility

Brazil agrees with the basic principle according to which "every internationally wrongful act of a State entails the international responsibility of that State".[27] This is a customary norm that has been confirmed by international tribunals on several occasions[28] and that has been codified by the International Law Commission (ILC). According to customary international law, as codified by the ILC, an internationally wrongful act is an action or omission that is attributable to a state and constitutes a breach of its international obligations.[29] By analogy, if a cyber operation attributable to a state breaches its international obligations, the state is responsible for this internationally wrongful act.

While many norms on state responsibility are generally considered customary international law, as reflected in the articles emanated from the ILC, there are other rules whose legal status is still unclear. The General Assembly took note of the ILC articles on state responsibility for internationally wrongful acts in its Resolution 56/83 of 2001. It has also commended the articles to the attention of governments without prejudice to the question of their future adoption. The ILC articles on state

[25] ICJ, Nicaragua, p. 105.

[26] ICJ, Oil Platform, p. 196-197.

[27] ILC, Articles on State Responsibility for Internationally Wrongful Acts, article 1.

[28] ICJ, Corfu Channel Case, Judgment, p. 23.

[29] ILC, Articles on State Responsibility for Internationally Wrongful Acts, article 2; PCIJ, Phosphates in Morocco, Judgment, p. 28.

responsibility have been under consideration of the General Assembly for 18 years, and the debates on this issue at its Sixth Committee demonstrate that states have divergent views on their legal status.

States and international courts have consistently recognized some of the ILC articles on state responsibility as customary international law, such as the rules for attribution. In the absence of any *lex specialis* for cyberspace, the customary norms concerning the attribution of conduct to a State are also applicable to the State's use of ICTs. Hence, cyber operations are attributable to a State if they are conducted by a State organ,[30] by persons or entities exercising elements of governmental authority,[31] or by persons or groups "acting on the instructions of, or under the direction or control of,"[32] the State. Regarding the latter criteria, for a private person or entity's conduct be attributable to a State, it has to be proved that the state had "effective control" over the operations.[33] It is clear, therefore, that a connection "must exist between the conduct of a [state] and its international responsibility."[34]

The technical difficulties in tracing cyber operations and in determining its authorship may lead to additional challenges in attributing an internationally wrongful act to a State. However, these added difficulties must not serve as a justification to lower the bar for determinations on attribution, which must be substantiated.

On the other hand, there are questions on the customary status of other set of articles on state responsibility emanated from the ILC, such as the ones on countermeasures. There are different views on the existence of widespread state practice and *opinio juris* capable of giving rise to customary international law on the legality and the requirements of countermeasures. Furthermore, it is generally accepted that the ILC provisions on countermeasures went beyond the codification of customary norms and had a strong element of progressive development of international law.[35] In this regard, it is important to recall that several states have criticized countermeasures because they would be prone to abuses, especially due to the material inequality of states.[36]

Particularly on ICTs, there are many factors advising a cautious approach on countermeasures. First, there is an added difficulty to attribute cyber activities to a particular State, which is aggravated by the fact that States have different technical resources and capabilities to both identify the origins of a cyber activity and to verify claims of breaches of international obligations through cyber means. Second, cyber operations can be designed to mask or spoof the perpetrator, which in turns increase the risks of miscalculated responses against innocent actors. Finally, the speed with which the precipitating wrongful cyber operations may unfold poses a high risk of escalation, with potential rippling effects to the kinetic domain.

With this in mind, Brazil considers that there needs to be further discussions on the legality of countermeasures as a response to internationally wrongful acts,

[30] ILC, Articles on the Responsibility of States for Internationally Wrongful Acts, art. 4.

[31] ILC, Articles on the Responsibility of States for Internationally Wrongful Acts, art. 5

[32] ILC, Articles on the Responsibility of States for Internationally Wrongful Acts, art. 8.

[33] ICJ, Nicaragua, Judgment, para 86 ; ICJ, Bosnian Genocide (2007), p. 208-211.

[34] ICJ, Bosnian Genocide (2007), p. 210.

[35] Max Planck Encyclopedia of International Law, Countermeasures (2015).

[36] See, e.g., A/C.6/51/SR.34 and A/C.6/55/SR.18.

including in the cyber context. The discussions must fully take into account the UN Charter in its entirety, thus excluding from the outset any possibility of using force as a countermeasure – a view that has already been confirmed by the ILC. The priority of peaceful settlement of disputes, in line with articles 2(3) and 33 of the UN Charter, must also be reaffirmed.

5. International Humanitarian Law

International humanitarian law (IHL) is fairly equipped to answer many of the questions associated with new technologies, including ICTs. There is no doubt that IHL applies to States use of ICTs during an armed conflict. The fact that a specific weapon has been invented after the development of humanitarian law does not exempt it from regulation. Quoting from the ICJ Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, excluding cyber operations from IHL scope of application "would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."[37]

IHL applies to situations amounting to armed conflict independently of its classification as such by the parties.[38] For IHL, it does not matter whether the armed conflict is lawful or not, because its objective is to minimize human suffering and provide a minimum level of protection to civilians in any scenario of hostilities. Hence, the recognition that international humanitarian law applies to the cyberspace does not in any way endorse its militarization or legitimize cyberwarfare, but only ensures a minimum level of protection if an armed conflict arises.

There are two instances where IHL might apply to cyber activities. First, if they are carried out as part of an ongoing armed conflict, contributing to conventional operations conducted by the parties. Second, if the cyber activities themselves cross the threshold of violence to be characterized as an armed conflict.

Of particular importance, the 2015 GGE report has noted the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction.

For Brazil, the IHL principle of precaution is also applicable to the use of ICTs by States, meaning that parties must "take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects".[39]

Moreover, according to AP I, States have an obligation, "in the study, development, acquisition or adoption of a new weapon, means or method of warfare," to "determine whether its employment would, in some or all circumstances," be prohibited.[40] This norm, although being less strict than some States wished during the negotiations of AP I,[41] already encompasses some precautionary elements. It must guide the development, acquisition and adoption of cyber capabilities.

---

[37] ICJ, Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, p. 259.

[38] Common article 2 to the Geneva Conventions of 1949.

[39] Additional Protocol I to the Geneva Conventions, art. 57.

[40] Additional Protocol I, art. 36.

[41] ICRC Commentary of 1987, API, art. 36.

In making the assessment of necessity, distinction, proportionality and precaution, parties must take into consideration the particularities of the cyberspace, such as the interconnectivity between military and civilian networks. The principle of distinction determines that cyberattacks must target military objectives and must not be indiscriminate. In case of doubt whether a cyber infrastructure that is normally dedicated to civilian purposes is being used to make an effective contribution to military action, it shall be presumed not to be so used.[42]

While holding the view that IHL applies to cyberspace, there are issues that deserve further reflection, such as the definition of cyberattack for the purposes of article 49 of AP I; the consideration of civilian data as a civilian object that entails protection under IHL; and when a civilian acting in the cyberspace might be considered as taking direct part in hostilities.

In any event, where IHL is silent or ambiguous, the "Martens clause" remains applicable,[43] ensuring that, in cases not covered by existing rules, "civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience".[44]

[42] Additional Protocol I, art. 52.

[43] ICJ, Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, p. 260.

[44] Additional Protocol I, art. 1.

Estonia

[Original: English]

Estonia welcomes the opportunity to submit its national contribution on the subject of how international law applies to the use of information and communications technologies (ICTs) by states as an annex to the report of the UN Group of Governmental Experts, as requested by UN General Assembly Resolution 73/266.

Estonia reiterates that existing international law applies in cyberspace. The rights and obligations set out in international law, including the UN Charter in its entirety, customary international law, international humanitarian and human rights law, apply to the use of ICTs by states. This means that international law applies to relations between states in cyberspace as it does in conventional domains of state interaction. To promote peace and stability in cyberspace and prevent conflict, it is necessary to have clear rules of responsible state behaviour in place.

Existing international law provides a solid normative framework for state actions, regardless of the means or the environment for these actions. The applicability of international law in cyberspace has been affirmed by the UN General Assembly endorsements of the 2013 and 2015 UN Group of Governmental Experts (GGE) consensus reports[45] and reaffirmed by the OEWG consensus report.[46] The current rules are technologically neutral and underline that state behaviour and the deployment of new transformative technologies do not change the applicability of international law.

States should strive to deepen a common understanding of how international law applies in cyberspace, alongside its possible implications and legal consequences. It is important to analyse how existing rules apply before discussing the need for any new agreement. Estonia sees notions for a new legally binding instrument as premature. From our perspective, current legal measures are sufficient to offer guidance on responsible state behaviour in cyberspace.

The 2013 and 2015 GGEs made substantive progress in terms of discussions on relevant legal rules and principles. In order to maintain peace and stability and promote an open, secure, peaceful and accessible cyberspace, we reiterate the following non-exhaustive elements: international law, including the UN Charter in its entirety, applies to state conduct in cyberspace, noting the principles of humanity, necessity, proportionality and distinction as well as respect for human rights and fundamental freedoms; states must meet their international obligations regarding internationally wrongful acts attributable to them under international law; states must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts; states must observe, among other principles of international law, sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States; the inherent right of States to take measures consistent with international law and as recognized in the Charter.

Alongside international law, voluntary, non-binding norms of responsible state behaviour can help prevent conflict in the ICT environment, reduce risks to international peace, security and stability and provide essential guidance for

[45] A/68/98*, adopted by UN General Assembly resolution A/RES/68/243; A/70/174, adopted by UN General Assembly resolution A/RES/70/237.

[46] A/75/816, adopted by UN General Assembly Decision A/DEC/75/564.

responsible state behaviour in cyberspace. Estonia underlines the importance of adhering to the set of voluntary non-binding norms reaffirmed in the UN General Assembly resolution 70/237. Together with confidence-building measures and capacity building measures, international law and norms constitute the framework for responsible state behaviour in cyberspace. We highlight that norms do not replace or alter States' obligations or rights under international law.

The paper first provides an overview of state obligations, followed by our position on state responsibility and attribution, and concludes with possible response options.

I. Obligations of states

Respect for sovereignty

Sovereignty as a fundamental principle of international law applies in cyberspace.

The 2013 and 2015 GGE consensus reports underscore that sovereignty and the international norms and principles that flow from it apply to state conduct of ICT-related activities. In addition, the 2013 GGE emphasised the importance of international law, the Charter of the UN and the principle of sovereignty as the basis for the use of ICTs by states.

States have territorial sovereignty over the ICT infrastructure and persons engaged in cyber activities on their territory. However, states' right to exercise sovereignty on their territory is not unlimited; states must respect international law, including human rights obligations. States also bear the responsibility to comply with legal obligations flowing from sovereignty – for example, the responsibility not to breach the sovereignty of other states and to take reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states. The principle of sovereignty is also closely linked with the principle of non-intervention and the principles of the prohibition of the threat or use of force.

The violation of sovereignty through cyber means can breach international law, and therefore may give the victim state the right to take measures, including countermeasures. Views on what constitutes a breach of sovereignty in cyberspace differ. Malicious cyber operations can be complex, cross several jurisdictions and may not always produce physical effects on targeted infrastructure.

Non-intervention

The principle of non-intervention is a well-established rule of international law, which flows from the principle of sovereignty, and applies to state conduct in cyberspace.

If an operation attributable to another state affects a state's internal or external affairs in such a manner that it coerces a state to take a course of action it would not voluntarily seek, it would constitute a prohibited intervention.

When discussing if a cyber operation constitutes an unlawful intervention into the external or internal affairs of another state, the element of coercion is a key factor. The possibility for a cyber operation to constitute an unlawful intervention in the functions that form a part of a state's *domaine réservé* has found acceptance among states, including Estonia, especially regarding the rights and obligations deriving from the principle of state sovereignty. States' *domaine réservé* according to the ICJ includes the "choice of a political, economic, social, and cultural system, and the

formulation of foreign policy."[47] Stemming from that, cyber operations that aim to force another nation to act in an involuntary manner or to refrain from acting in a certain manner, and target the other nation's *domaine réservé* (e.g. national democratic processes such as elections, or military, security or critical infrastructure systems) could constitute such an intervention.

Prohibition of the use of force

States must refrain in their international relations from carrying out cyber operations which, based on their scale and effect, would constitute a threat or use of force against the territorial integrity or a political independence of any state, or in any other manner inconsistent with the purposes of the UN.

While taking measures in cyberspace, states must comply with the obligations and constraints enshrined in international law, including the UN Charter and customary international law. The threat or use of force in international relations is prohibited; however, the UN Charter foresees concrete situations where it could be allowed (in response to an armed attack, as self-defence or in accordance with chapter VII of the UN Charter).

The prohibition of the threat or use of force in cyberspace was also acknowledged and highlighted in the 2015 GGE report, endorsed by the UN General Assembly. Notably, the report states that "in considering the application of international law to State use of ICTs, the GGE identified as of central importance the commitments of States to the following principles of the Charter and other international law […] refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State […]."[48].

A cyber operation that targets critical infrastructure and results in serious damage, injury or death, or a threat of such an operation, would be an example of use of force.

Due diligence

The due diligence obligation of a state not to knowingly allow its territory to be used for acts that adversely affect the rights of other states has its legal basis in existing international law and applies as such in cyberspace.

The due diligence obligation derives from the principle of sovereignty. A state has the exclusive right to control activities within its territory. At the same time, this means that it is also obliged to act when its territory is used in a manner that adversely affects the rights of other states.

Without this obligation, international law would leave injured states defenceless in the face of malicious cyber activity that emanates from other states' territories. This is particularly relevant when state responsibility cannot be established. Therefore, states have to make reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states. Such reasonable efforts are relative to national capacity as well as the availability of and access to information. Meeting this

[47] Nicaragua case: www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

[48] A/70/174, adopted by UN General Assembly resolution A/RES/70/237.

expectation encompasses taking all feasible measures in order to end the ongoing malicious cyber activity.

Estonia is at the position that the obligation of due diligence requires consideration of the technical, political and legal capacities of a state. In addition, due diligence is related to taking action by applying all lawful and feasible measures in order to halt an ongoing malicious cyber operation. States should strive to develop means to offer support, when requested by the injured state, to identify or attribute malicious cyber operations. These actions could for example include warning, cooperating and sharing relevant data pertaining to an incident, investigating the incident and prosecuting the perpetrators, assisting the victim state(s) or accepting assistance. The necessary measures depend on the incident and are applied on a case-by-case basis.

International humanitarian law

If a situation amounts to an armed conflict and cyber operations are carried out during that conflict, international humanitarian law applies to these cyber operations as it does to all operations with a nexus to armed conflict in general.

Estonia believes that international humanitarian law sets boundaries for states' activities in conflict, protecting civilian persons and infrastructure, and acting as a constraint, not a facilitator of conflict.

In our view, international humanitarian law provides the necessary rules constraining states' conduct in conflict that also extend to cyber operations. Its applicability does not lead to the militarisation of cyberspace.

Armed conflicts today and in the future may involve offensive cyber capabilities. Therefore, it is vital that the use of such capabilities would be subject to obligations deriving from international humanitarian law, including taking into account such considerations as humanity, necessity, proportionality and distinction.

International human rights law

All states bear an obligation to ensure and protect fundamental rights and freedoms both online as well as offline.

In regards to state use of ICTs, states must comply with Human Rights obligations including those deriving from the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Cybersecurity and human rights are complementary, mutually reinforcing and interdependent. Both need to be pursued together to effectively promote freedom and security. Cybersecurity laws, policies and practices must not be used as a pretext to silence human rights defenders and restrict human rights and fundamental freedoms in general.

The prevention, mitigation of as well as responses to cyber incidents should not violate human rights. This in particular includes the freedom of expression, the freedom to seek, receive and impart information, the freedom of peaceful assembly and association, and the right to privacy.

As a founding member of Freedom Online Coalition (FOC) Estonia nationally and internationally supports policies and practices that promote the protection of human rights and fundamental freedoms online.[49]

Public authorities have a duty to respect and protect the freedom of expression and the freedom to seek, receive and impart information. Estonia is a proponent of transparency in government processes – transparency is essential in order for citizens to be able to trust the e-services provided to them. In addition, the development of e-government solutions in the public sector has to go hand in hand with safeguarding the privacy of citizens and the security of their data.

II. State responsibility and attribution

State responsibility

The law of state responsibility is a cornerstone for responsible state behaviour in cyberspace when it comes to assessing the unlawfulness of cyber operations below the threshold of use of force.

The law of state responsibility includes key principles that govern when and how a state is held responsible for cyber operations that constitute a breach of international obligation, by either an act or an omission. A cyber operation can constitute an internationally wrongful act if it is attributable under international law and it constitutes a breach of international obligation under the law of state responsibility. States must comply with customary international law mirrored in the Articles for Responsibility of States for Internationally Wrongful Acts.

States are responsible for their activities in cyberspace. States are accountable for their internationally wrongful cyber operations just as they would be responsible for any other activity according to international treaties or customary international law. State responsibility applies regardless of whether such acts are carried out by a state or non-state actors instructed, directed or controlled by a state.

States cannot waive their responsibility by carrying out malicious cyber operations via non-state actors and proxies. For example, if a hacker group launches cyber operations which have been tailored according to instructions from a state, or the cyber operations are directed or controlled by that state, state responsibility can be established.

Attribution

A cyber operation is deemed an internationally wrongful act when it is attributable to a state under international law and involves a breach of an international obligation of the state.

Attribution remains a national political decision based on technical and legal considerations regarding a certain cyber incident or operation. Attribution will be conducted on a case-by-case basis, and various sources as well as the wider political, security and economic context can be considered.

[49] Freedom Online Coalition statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies (2020): https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf.

According to Article 2(a) of ARSIWA, an internationally wrongful act of a state has taken place when the conduct consisting of an action or omission is attributable to a state and the action or omission is wrongful under international law. Attribution allows establishing if a malicious cyber operation is linked with a state in order to invoke the responsibility of that state.

A state as a subject of international law can exercise its rights and obligations through its organs and in some instances by natural and legal persons. The attribution of an internationally wrongful act, including an internationally wrongful cyber operation, requires careful assessment of whether and how malicious activity conducted by a person, a group of persons or legal persons can be considered as the act of a state. In principle, both acts and omissions are attributable to states.

Attribution is closely related to the availability of information of the malicious cyber operation. Following the various necessary assessments, public statements on attribution can be made, with the aim of increasing accountability in cyberspace and emphasising the importance of adhering to international law obligations and norms of responsible state behaviour.

III. State's response

In order to enforce state responsibility, states maintain all rights to respond to malicious cyber operations in accordance with international law. If a cyber operation is unfriendly or violates international law obligations, injured states have the right to take measures such as retorsions, countermeasures or, in case of an armed attack, the right to self-defence. These measures can be either individual or collective. The main aim of reactive measures in response to a malicious cyber operation is to ensure responsible state behaviour in cyberspace and the peaceful use of ICTs.

Peaceful settlement of disputes

It is an obligation for states to settle their international disputes that endanger international peace and security by peaceful means.

As outlined in the UN Charter, possible solutions to settle disputes between states include negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, and other internationally lawful action.

In accordance with the UN Charter Chapter VI, the UN Security Council may also call upon the parties, when it deems necessary, to settle their dispute by such peaceful means. In specific cases with respect to cyber activities endangering international peace and security, the other powers and responsibilities of the UN Security Council outlined in the UN Charter may be exercised in order to maintain and restore international peace and security.

The obligation to seek peaceful settlement of disputes does not preclude a state's inherent right for self-defence in response to an armed attack, the right for taking lawful countermeasures, or other lawful action.

Retorsion

Retorsions may be taken as a response to malicious cyber operations as long as they are not in violation with international law.

Retorsions will remain as measures for a state to respond to unfriendly acts or violations of international law, which by themselves do not constitute a countermeasure. States have the right to apply these measures as long as they do not violate obligations under international law.

These measures could, for example include the expulsion of diplomats or applying restrictive measures to officials of a third country such as asset freezes or travel bans. One example of such a mechanism would be the European Union's cyber sanctions regime and cyber diplomacy toolbox, which offer an array of measures that could be taken as a response to malicious cyber operations.[50]

Countermeasures

If a cyber operation does not reach the threshold of armed conflict but nonetheless constitutes a violation of international law, states maintain the right to take countermeasures, in accordance with the law of state responsibility.

Countermeasures have strict legal criteria – an injured state may only take countermeasures against a state that is responsible for an internationally wrongful act in order to induce the given state to comply with its international obligations. This means that under certain circumstances, an injured state has the right to take measures that would normally violate international customary law or international treaties, but taken as a countermeasure such actions would be permitted as they would be in response to a violation of international law.

In order to take countermeasures in response to a malicious cyber operation violating international law, the operation in question must have been attributed to a state.

Right to self-defence

In accordance with Article 51 of the UN Charter, states have the right for self-defence in the case of an armed attack.

In order to assess if a cyber operation reaches the threshold of the use of force or an armed attack based on Article 2(4) or 51 of the UN Charter, we must consider the scale and effects of the operation. If the effects of a cyber operation are comparable to a kinetic attack, it could constitute an armed attack.

In such a situation, the injured state has the right to self-defence considering all applicable restrictions of the UN Charter and customary international law, such as proportionality and necessity.

In its response to an armed attack by cyber means, the injured state is not necessarily limited to taking measures by cyber means – all means remain reserved to states in order to respond to an armed attack in a manner that is proportionate and in accordance with other provisions of international law.

[50] Draft Council of the European Union Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") (2017): https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf; Council of the European Union Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States (2019): https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf.

Estonia believes that cyber operations that cause injury or death to persons, damage or destruction could amount to an armed attack under the UN Charter.

IV. Conclusions

International law remains essential to relations between states for setting clear boundaries on what is and is not acceptable behaviour in cyberspace. Alongside other elements of the cyber stability framework, international law provides overarching guidance as to states' international rights and obligations applicable to cyberspace.

A clear need for deepening the understanding on how international law applies to cyberspace has been noted during discussions between states. We welcome the publication of expert and national views and work done by states as well as other stakeholders, including academia and relevant organisations.[51]

Estonia is looking forward to further constructive exchanges of views, including under the auspices of the UN, on how international law applies to state use of ICTs. The UN is an inclusive and necessary format to enable substantive discussions on responsible state behaviour in cyberspace. States should also engage with all stakeholders, including the private sector, civil society and academia, to discuss international law issues. One possible and helpful avenue for further awareness raising on how existing international law applies in cyberspace could be as part of a permanent Programme of Action (PoA) under the auspices of the UN First Committee.

[51] For example, the work done by the International Committee of the Red Cross on the application of international humanitarian law (IHL) to cyber operations during armed conflicts is commendable and can help with further study on how IHL principles apply in cyberspace.

Germany

[Original: English]

I. Introduction

Cyber activities have become an **integral part of international relations.** The vast interconnectedness of networks, technologies and cyber processes across borders has brought societies and individuals from different nations closer together and has opened up new opportunities for cooperation among both State and non-State actors. At the same time, States and societies have grown highly dependent on the functioning of IT infrastructures. This has created new vulnerabilities. In cyberspace, only limited resources are often needed to cause significant harm. This poses security threats for States and societies. Harmful cross-border cyber operations, both by State and non-State actors, can jeopardize international stability.

Germany is firmly convinced that **international law is of critical importance when dealing with opportunities and risks related to the use of information and communication technologies in the international context.** As a main pillar of a rules-based international order, international law as it stands provides binding guidance on States' use and regulation of information and communication technologies and their defence against malicious cyber operations. In particular, the UN Charter fulfils a core function with regard to the maintenance of international peace and security – also in relation to cyber activities. In this regard, Germany reemphasizes its conviction that **international law, including the UN Charter and international humanitarian law (IHL), applies without reservation in the context of cyberspace.**[52]

This paper discusses selected aspects of the interpretation of certain core principles and rules of international law in the cyber context.[53] Germany thereby aims to **contribute to the ongoing discussion** on the modalities of application of international law – most of which predates the development and rise of information and communication technologies – in the cyber context. The paper also intends to foster **transparency, comprehensibility and legal certainty** with regard to an important aspect of foreign affairs. The explanations take into account, *inter alia,* the 2013 and 2015 reports of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.[54] They are based on applicable international law and in this regard consider, to a significant degree, the findings of independent international law experts recorded in the Tallinn Manual 2.0.[55]

---

[52] See also United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, report of 24 June 2013, UN Doc. A/68/98, para. 19 and cf. report of 22 July 2015, UN Doc. A/70/174, paras. 24, 25; General Assembly resolution 70/237, Developments in the field of information and telecommunications in the context of international security, UN Doc. A/RES/70/237, 30 December 2015.

[53] The choice of rules and principles discussed is necessarily selective and no conclusions regarding Germany's legal position can be drawn from any actual or perceived omission to mention certain rules, principles, criteria or legal considerations.

[54] See above, note 52.

[55] Schmitt, M. (gen. ed.)/Vihul, L. (man. ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, 2nd edition, Cambridge University Press 2017. The Tallinn Manual 2.0 is a paper created by independent experts and constitutes neither a document stating

For the purpose of this paper, ‘cyber processes’ are events and sequences of events of data creation, storage, processing, alteration or relocation through means of information technology. The term ‘cyber infrastructure’ refers to all types of hardware and software components, systems and networks which allow for the implementation of ‘cyber processes’. This includes ‘[t]he communications, storage, and computing devices upon which information systems are built and operate.’[56] ‘Cyber activities’ are ‘cyber processes’ instigated by users of cyber infrastructure. The term ‘cyber operation’ more narrowly refers to the ‘employment of cyber capabilities to achieve objectives in or through cyberspace.’[57] ‘Cyberspace’ itself is understood here as the conglomerate of (at least partly interconnected) ‘cyber infrastructures’ and ‘cyber processes’ in the above-mentioned sense. In this paper, the adjective ‘malicious’, when used to describe certain activities in cyberspace, is not purported to carry a technical legal meaning.

II. Obligations of States derived from the United Nations Charter

a) Sovereignty

The legal principle of **State sovereignty**[58] **applies to States’ activities with regard to cyberspace.**[59] State sovereignty implies, *inter alia,* that a State retains a right of regulation, enforcement and adjudication (jurisdiction) with regard to both persons engaging in cyber activities and cyber infrastructure on its territory.[60] It is limited only by relevant rules of international law, including international humanitarian law and international human rights law. Germany recognizes that due to the high degree of cross-border interconnectedness of cyber infrastructures, a State’s exercise of its jurisdiction may have unavoidable and immediate repercussions for the cyber infrastructure of other States.[61] While this does not limit a State’s right to exercise its jurisdiction, **due regard has to be given to potential adverse effects on third States**.

By virtue of sovereignty, a State’s **political independence** is protected and it retains the right to freely choose its political, social, economic and cultural system. *Inter alia,* a State may generally decide freely which role information and communication technologies should play in its governmental, administrative and adjudicative proceedings. Foreign interference in the conduct of elections of a State may under certain circumstances constitute a breach of sovereignty or, if pursued by

---

NATO positions nor a position paper by States. In the following, references to the Tallinn Manual 2.0 are made for information purposes only and do not necessarily constitute an endorsement of the referenced text by the German government.

[56] Tallinn Manual 2.0 (note 55), Glossary (p. 564).

[57] Ibid.

[58] The legal principle of State sovereignty is enshrined – in conjunction with the notion of equality of States – in Art. 2 para. 1 of the UN Charter.

[59] See also UN Group of Governmental Experts, reports of 2013 and 2015 (note 52), paras. 20 and 27, 28 (b) respectively; Tallinn Manual 2.0 (note 55), rule 1.

[60] A State’s jurisdiction may under certain conditions apply to situations beyond its borders, i.e. according to the principles of active and of passive nationality as well as universality.

[61] For example, restrictive regulatory or enforcement activities regarding important internet nodes in the territory of one State may seriously impair the functioning of networks of other States.

means of coercion, of the prohibition of wrongful intervention.[62] Moreover, by virtue of its sovereignty, a State may decide freely over its foreign policy also in the field of information and communication technologies.[63]

Furthermore, a State's **territorial sovereignty** is protected. Due to the rootedness of all cyber activities in the actions of human beings using physical infrastructure, cyberspace is not a deterritorialized forum.[64] In this regard, Germany underlines that there are no independent 'cyber borders' incongruent with a State's physical borders which would limit or disregard the territorial scope of its sovereignty. Within its borders, a State has the exclusive right – within the framework of international law – to fully exercise its authority, which includes the protection of cyber activities, persons engaging therein as well as cyber infrastructures in the territory of a State against cyber and non-cyber-related interferences attributable to foreign States.[65]

As a corollary to the rights conferred on States by the rule of territorial sovereignty, States are under an 'obligation not to allow knowingly their territory to be used for acts contrary to the rights of other States'[66] – this generally applies to such use by State and non-State actors. The **'due diligence principle',** which is widely recognized in international law, is applicable to the cyber context as well and gains particular relevance here because of the vast interconnectedness of cyber systems and infrastructures.

Germany agrees with the view that **cyber operations attributable to States which violate the sovereignty of another State are contrary to international law.**[67] In this regard, State sovereignty constitutes a legal norm in its own right and may apply directly as a general norm also in cases in which more specific rules applicable to State behaviour, such as the prohibition of intervention or the use of force, are not applicable. Violations of State sovereignty may *inter alia* involve its territorial dimension; in this regard, the following categories of cases may be relevant (without excluding the possibility of other cases):

Germany essentially concurs with the view proffered, *inter alia,* in the Tallinn Manual 2.0 that cyber operations attributable to a State which lead to **physical effects and harm in the territory of another State** constitute a violation of that State's territorial sovereignty.[68] This encompasses physical damage to cyber infrastructure components *per se* and physical effects of such damage on persons or on other infrastructure, i.e. cyber or analogue infrastructure components connected to the damaged cyber component or infrastructure located in the vicinity of the damaged cyber infrastructure (provided a sufficient causal link can be established).

---

[62] See below, at 0.

[63] See Tallinn Manual 2.0 (note 55), rule 3 ('external sovereignty').

[64] Ibid., rule 1, commentary, para. 5.

[65] Ibid., rule 2 with commentary, para. 2.

[66] See International Court of Justice (ICJ), Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania), Judgement of 9 April 1949, I.C.J. Reports 1949, 4, 22; Permanent Court of Arbitration (PCA - administering institution), Island of Palmas Case (or Miangas), United States of America v. The Netherlands, Arbitral Award (M. Huber) of 4 April 1928, (1928) II RIAA 829, 839.

[67] Cf. Tallinn Manual 2.0 (note 55), rule 4.

[68] Tallinn Manual 2.0 (note 55), rule 4, commentary, para. 11.

Germany generally also concurs with the view expressed and discussed in the Tallinn Manual 2.0 that certain effects in form of **functional impairments** with regard to cyber infrastructures located in a State's territory may constitute a violation of a State's territorial sovereignty.[69] In Germany's view, this may also apply to certain substantial non-physical (i.e. software-related) functional impairments. In such situations, an evaluation of all relevant circumstances of the individual case will be necessary. If functional impairments result in substantive secondary or indirect physical effects in the territory of the target State (and a sufficient causal link to the cyber operation can be established), a violation of territorial sovereignty will appear highly probable.[70]

In any case, **negligible** physical effects and functional impairments below a certain impact threshold cannot – taken by themselves – be deemed to constitute a violation of territorial sovereignty.

Generally, the fact that a piece of **critical infrastructure** (i.e. infrastructure which plays an indispensable role in ensuring the functioning of the State and its society) or a company of special public interest in the territory of a State has been affected may indicate that a State's territorial sovereignty has been violated. However, this cannot in and of itself constitute a violation, *inter alia* because uniform international definitions of the terms do not yet exist. Also, cyber operations in which infrastructures and/or companies which do not qualify as 'critical' or 'of particular public interest' are affected may likewise violate the territorial sovereignty of a State.

b) Prohibition of wrongful intervention

The prohibition of a wrongful intervention between States[71] is not explicitly mentioned in the UN Charter. However, it is a corollary of the sovereignty principle, can be derived from art. 2 para. 1 UN Charter and is grounded in customary international law. Generally, for State-attributable conduct to qualify as a wrongful intervention, the conduct must **(1) interfere with the *domaine réservé* of a foreign State and (2) involve coercion.**[72] Especially the definition of the latter element requires further clarification in the cyber context.

In its Nicaragua judgement, the International Court of Justice (ICJ) held that '[t]he element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.'[73] Malicious cyber activities will only in some cases amount to direct or indirect use of force.[74] However, measures below this threshold may also qualify as coercive. Generally, Germany is of the opinion that cyber measures may constitute a prohibited

[69] Cf. ibid., rule 4, commentary, para. 13 ("loss of functionality").

[70] Cf. ibid.

[71] On its applicability in the cyber context see also UN Group of Governmental Experts, report of 2015 (note 52), para. 28 (b).

[72] International Court of Justice (ICJ), Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America), Merits, Judgement of 27 June 1986, I.C.J. Reports 1986, 14, para. 205.

[73] Ibid.

[74] See below, at 0.

intervention under international law if they are **comparable in scale and effect to coercion in non-cyber contexts**.

Coercion implies that a State's internal processes regarding aspects pertaining to its *domaine réservé* are significantly influenced or thwarted and that its will is manifestly bent by the foreign State's conduct. However, as is widely accepted, **the element of coercion must not be assumed prematurely.** Even harsher forms of communication such as pointed commentary and sharp criticism as well as (persistent) attempts to obtain, through discussion, a certain reaction or the performance of a certain measure from another State do not as such qualify as coercion. Moreover, the acting State must intend to intervene in the internal affairs of the target State[75] – otherwise the scope of the non-intervention principle would be unduly broad.

In the context of wrongful intervention, the problem of **foreign electoral interference by means of malicious cyber activities** has become particularly virulent. Germany generally agrees with the opinion that malicious cyber activities targeting foreign elections may – either individually or as part of a wider campaign involving cyber and non-cyber-related tactics – constitute a wrongful intervention.[76] For example, it is conceivable that a State, by **spreading disinformation via the internet, may deliberately incite violent political upheaval, riots and/or civil strife** in a foreign country, thereby significantly impeding the orderly conduct of an election and the casting of ballots. Such activities may be comparable in scale and effect to the support of insurgents and may hence be akin to coercion in the above-mentioned sense. A detailed assessment of the individual case would be necessary.

Also, the **disabling of election infrastructure and technology** such as electronic ballots, etc. by malicious cyber activities may constitute a prohibited intervention, in particular if this compromises or even prevents the holding of an election, or if the results of an election are thereby substantially modified.

Furthermore, beyond the mentioned examples, cyber activities targeting elections may be comparable in scale and effect to coercion if they **aim at and result in a substantive disturbance or even permanent change of the political system of the targeted State,** i.e. by significantly eroding public trust in a State's political organs and processes, by seriously impeding important State organs in the fulfilment of their functions or by dissuading significant groups of citizens from voting, thereby undermining the meaningfulness of an election. Due to the complexity and singularity of such scenarios, it is difficult to formulate abstract criteria. Discussions in this context are still ongoing.

c) Prohibition of the use of force

So far, the vast majority of malicious cyber operations fall outside the scope of 'force'. However, **cyber operations might *in extremis* fall within the scope of the prohibition of the use of force** and thus constitute a breach of art. 2 para. 4 UN Charter.

The ICJ has stated in its Nuclear Weapons opinion that Charter provisions *'apply to any use of force, regardless of the weapons employed.'*[77] Germany shares the view

[75] Cf. Tallinn Manual 2.0 (note 55), rule 66, commentary, para. 27.

[76] See also above, 0.

[77] International Court of Justice (ICJ), Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, I.C.J. Reports 1996, 226, para. 39.

that with regard to the definition of ‘use of force’, emphasis needs to be put on the **effects rather than on the means** used.

Cyber operations can cross the threshold into use of force and cause significant damage in two ways. Firstly, they can be **part of a wider kinetic attack.** In such cases they are one component of a wider operation clearly involving the use of physical force, and can be assessed within the examination of the wider incident. Secondly, outside the wider context of a kinetic military operation, cyber operations can **by themselves cause serious harm and may result in massive casualties.**

With regard to the latter case, Germany shares the view expressed in the Tallinn Manual 2.0: the threshold of use of force in cyber operations is defined, in analogy to the ICJ’s Nicaragua judgement,[78] by the **scale and effects** of such a cyber operation.[79] Whenever scale and effects of a cyber operation are comparable to those of a traditional kinetic use of force, it would constitute a breach of art. 2 para. 4 UN Charter.

The determination of a cyber operation as having crossed the threshold of a prohibited use of force is a **decision to be taken on a case-by-case basis.** Based on the assessment of the scale and effects of the operation, the broader context of the situation and the significance of the malicious cyber operation will have to be taken into account. Qualitative criteria which may play a role in the assessment are, *inter alia,* the severity of the interference, the immediacy of its effects, the degree of intrusion into a foreign cyber infrastructure and the degree of organization and coordination of the malicious cyber operation.

III. Obligations of States under international humanitarian law (IHL)

a) Applicability of IHL in the cyber context

Germany reiterates its view that **IHL applies to cyber activities in the context of armed conflict.**[80] The fact that cyberspace as a domain of warfare was unknown at the time when the core treaties of IHL were drafted does not exempt the conduct of hostilities in cyberspace from the application of IHL. As for any other military operation, IHL applies to cyber operations conducted in the context of an armed conflict independently of its qualification as lawful or unlawful from the perspective of the *ius ad bellum.*

An **international armed conflict** – a main prerequisite for the applicability of IHL in a concrete case – is characterized by armed hostilities between States. This may also encompass hostilities that are partially or totally conducted by using cyber means. Germany holds the view that cyber operations of a non-international character, e.g. of armed groups against a State, which reach a sufficient extent, duration, or intensity (as opposed to acts of limited impact) may be considered a **non-international armed conflict** and thereby also trigger the application of IHL.[81]

---

[78] ICJ, Military and Paramilitary Activities in and against Nicaragua (note 72), para. 195.

[79] Tallinn Manual 2.0 (note 55), rules 69, 71.

[80] Cf. also ibid., rule 80.

[81] Generally, a non-international armed conflict is characterized by ‘protracted armed violence between governmental authorities and organized armed groups or between such groups within a State’, International Criminal Tribunal for the former Yugoslavia (ICTY), Prosecutor v. Dusko Tadić (aka ‘Dule’), Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Appeals Chamber),

At the same time, cyber actions can become **part of an ongoing armed conflict.** In order to fall within the ambit of IHL, the cyber operation must show a **sufficient nexus with the armed conflict,**[82] i.e. the cyber operation must be conducted by a party to the conflict against its opponent and must contribute to its military effort.[83]

Cyber operations between a non-State actor and a State alone *may* provoke a non-international armed conflict. However, this will only seldom be the case due to the level of intensity, impact and extent of hostilities required. Thus, activities such as a large-scale intrusion into foreign cyber systems, significant data theft, the blocking of internet services and the defacing of governmental channels or websites will usually not singularly and in themselves bring about a non-international armed conflict.[84]

b) The fundamental principles of IHL limiting the recourse to cyber operations in the context of an armed conflict

The basic principles governing the conduct of hostilities, including by cyber means, such as the principles of distinction, proportionality, precautions in attack and the prohibition of unnecessary suffering and superfluous injury, apply to cyber attacks in international as well as in non-international armed conflicts.

Germany defines a **cyber attack in the context of IHL as an act or action initiated in or through cyberspace to cause harmful effects on communication, information or other electronic systems, on the information that is stored, processed or transmitted on these systems or on physical objects or persons.**[85] The occurrence of physical damage, injury or death to persons or damage or destruction to objects comparable to effects of conventional weapons is not required for an attack in the sense of art. 49 para. 1 Additional Protocol I to the Geneva Conventions.[86] However, the mere intrusion into foreign networks and the copying of data does not constitute an attack under IHL.

1) The prohibition of indiscriminate attacks and cyber operations

The principle of distinction obliges States to differentiate between military and civilian objects, as well as between civilians, on the one hand, and combatants, members of organized armed groups and civilians taking direct part in hostilities, on the other hand. While IHL does not prohibit an attack on the latter, civilians (not taking direct part in hostilities) and civilian objects must be spared.

Civilians operating in cyberspace can be considered as taking direct part in hostilities with the result of losing their protection from attack and the effects of the hostilities, provided the following conditions are met: Their acts are likely to adversely affect the military operations or military capacity of a party, there is a direct causal link between their acts and the adverse effects and the acts are specifically designed to inflict harm in support of a party to an armed conflict and to the detriment

---

Case No. IT-94-1, 2 October 1995, para. 70. On the definitions of international and non-international armed conflict in the cyber context, cf. also Tallinn Manual 2.0 (note 55), rules 82 and 83.

[82] Tallinn Manual 2.0 (note 55), rule 80, commentary, para. 5.

[83] See on the discussion ibid., rule 80, commentary, paras. 5, 6.

[84] Ibid., rule 83, commentary, paras. 2, 7 and 8.

[85] See also NATO Terminology Tracking Form (TTF) 2015-0028 (last entry 2019-02-12).

[86] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3.

of another (belligerent nexus).[87] Thus, Germany agrees with the view that, for example, 'electronic interference with military computer networks […], whether through computer network attacks or computer network exploitation, as well as wiretapping […] [of an] adversary's high command or transmitting tactical targeting information for an attack', could suffice in order to consider a civilian person as directly participating in hostilities.[88]

Following the same logic, a **civilian object like a computer, computer networks, and cyber infrastructure, or even data stocks,** can become a military target, if used either for both civilian and military purposes or exclusively for the latter. However, in cases of doubt, the determination that a civilian computer is in fact used to make an effective contribution to military action may only be made after a careful assessment.[89] Should substantive doubts remain as to the military use of the object under consideration, it shall be presumed not to be so used.[90]

The benchmark for the application of the principle of distinction is the **effect caused by a cyber attack,** irrespective of whether it is exercised in an offensive or a defensive context. Thus, **computer viruses designed to spread their harmful effects uncontrollably** cannot distinguish properly between military and civilian computer systems as is required under IHL and their use is therefore prohibited as an indiscriminate attack. In contrast, **malware that spreads widely into civilian systems but damages only a specific military** target does not violate the principle of distinction. Given the complexity of cyber attacks, the limited options to comprehensively appraise their nature and effects and the high probability of an impact on civilian systems, having recourse to the appropriate expertise to assess potential indiscriminate effects throughout the mission planning process is of key importance to Germany.

A cyber attack directed against a military target which is nevertheless expected to cause **incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof,** is also prohibited under IHL if such incidental effects would be excessive in relation to the concrete and direct military advantage anticipated.[91] If a cyber attack is executed in conjunction with other forms of military action, such as attacks with conventional weapons directed against the same installation, the military advantage and the collateral damage must be considered with regard to the 'attack […] as a whole and not only […] [with regard to] isolated or particular parts of the attack.'[92]

Assessing collateral damage and incidental injury or loss of life when conducting a proportionality analysis can be even more difficult in the context of

---

[87] International Committee of the Red Cross (ICRC)/Melzer, N., Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law, 2009, available at www.icrc.org, p. 16.

[88] Ibid., p. 48 (footnotes omitted).

[89] Tallinn Manual 2.0 (note 55), rule 102.

[90] Additional Protocol I (note 86), art. 52 para. 3.

[91] Additional Protocol I (note 86), art. 51 para. 5 (b); Tallinn Manual 2.0 (note 55), rule 113.

[92] Declarations made by Germany at the time of ratification of Additional Protocol I (note 86), see 'Bekanntmachung über das Inkrafttreten der Zusatzprotokolle I und II zu den Genfer Rotkreuz-Abkommen von 1949' (Notice concerning the entry into force of Additional Protocols I and II to the 1949 Geneva Red Cross Conventions), 30 July 1991, BGBl. 1991 II, 968, 969; Tallinn Manual 2.0 (note 55), rule 113, commentary, para. 10.

cyber operations as compared to more traditional, i.e. physical, means or methods of warfare. This however does not discharge those planning and coordinating attacks from taking into account their foreseeable direct and indirect effects.

2) The obligation to take precaution in planning and executing a cyber attack

A corollary to the prohibition of indiscriminate cyber attacks is the duty to take constant care to spare the civilian population, civilians and civilian objects during hostilities involving cyber operations.[93]

Those who plan, approve or execute attacks must take **all feasible precautions in the choice of means and methods** with a view to avoiding, and in any event minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects.[94] This might encompass **gathering intelligence on the network in question** through mapping or other processes in order to assess the attack's likely effects. Also, the **inclusion of a deactivation mechanism** or a specific configuration of the cyber tool which limits the effects on the intended target might be considered. Moreover, if it becomes apparent that the target is not a military one or is subject to special protection, those who plan, approve or execute the cyber attack must refrain from executing or suspend the attack. The same applies when the attack may be expected to cause excessive collateral damage to civilians and civilian objects.[95]

The obligation to take precautions in attack is complemented by the **obligation to conduct weapon reviews of any new means or method of cyber warfare** to determine whether its employment would, in some or in all circumstances, be prohibited by international law.[96] The findings of such reviews, to the extent that they identify legal constraints for the employment of means and methods in particular operational settings, should serve as a basis for operational planning. However, the means and methods used in cyber warfare are typically tailored to their targets, as they generally involve exploiting vulnerabilities that are specific to the target and the operational context. This entails that the development of means or the adoption of the method will often coincide with the planning of a concrete operation. Thus, the obligation to take precautions in attack and the requirement of a legal review remain separate requirements, but may overlap in substance.

IV) States' response options

a) Attribution

Attributing a cyber incident is of critical importance as a part of holding States responsible for wrongful behaviour and for documenting norm violations in cyberspace. It is also a prerequisite for certain types of responsive action. As regards the attribution of certain acts to States under international law, Germany applies the relevant **customary law rules on State responsibility also to acts in cyberspace,** subject to any *lex specialis* provisions. *Inter alia,* cyber operations conducted by **State**

[93] Additional Protocol I (note 86), art. 57 para. 1; Tallinn Manual 2.0 (note 55), rule 114.

[94] Cf. Additional Protocol I (note 86), art. 57 para. 2 (a) (ii); Tallinn Manual 2.0 (note 55), rule 116.

[95] Additional Protocol I (note 86), art. 57 para. 2 (a) (iii); art. 57 para. 2 (b); Tallinn Manual 2.0 (note 55), rules 117, 119.

[96] In Germany, the legal review is carried out by the steering committee for the review of new weapons and methods of warfare under the direction of the Directorate-General for Legal Affairs, Joint service regulation A 2146/1.

organs are attributable to the State in question.[97] The same applies with regard to **persons or entities which are empowered by the law of a State to exercise elements of the governmental authority** and act in that capacity in the particular instance.[98] Attribution is not excluded because such organ, person or entity acting in an official capacity exceeds its authority or contravenes instructions – cyber operations conducted ***ultra vires*** are likewise attributable to the State in question.[99] This applies *a maiore ad minus* when only parts of an operation are *ultra vires*.

Generally, the mere (remote) use of cyber infrastructure located in the territory of a State (forum State) by another State (acting State) for the implementation of malicious cyber operations by the latter does not lead to an attribution of the acting State's conduct to the forum State. However, the forum State may under certain circumstances incur responsibility on separate grounds, for example if its conduct with regard to another State's use of its cyber infrastructure for malicious purposes qualifies as **aid or assistance.**[100] This *inter alia* applies if the forum State actively and knowingly provides the acting State with access to its cyber infrastructure and thereby facilitates malicious cyber operations by the other State.[101]

Moreover, cyber operations conducted by **non-State actors which act on the instructions of, or under the direction or control of, a State** are attributable to that State.[102] The same principles apply as in the physical world: if a State recurs to private actors in order to commit an unlawful deed, the actions by the private actor will regularly be attributable to the State. States should recognize that they are accountable for the actions of proxies acting under their control.[103] The State must have control over a specific cyber operation or set of cyber operations conducted by the non-State actor. While a sufficient degree or intensity of such control is necessary, the State is **not required to have detailed insight into or influence over all particulars, especially those of a technical nature, of the cyber operation.** A comprehensive assessment of the circumstances of the individual case will be necessary to establish an attributive link.[104]

Beyond the mentioned situations of attribution and aid and assistance, a State may also become liable under international law in connection with another State's or a non-State actor's actions if the first State fails to abide by its obligations stemming from the 'due diligence' principle.[105]

---

[97] Cf. International Law Commission (ILC), Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001, in: Report of the International Law Commission on the work of its fifty-third session, 23 April – 1 June and 2 July – 10 August 2001, Official Records of the General Assembly, Fifty-sixth Session, Supplement No. 10, UN Doc. A/56/10, 26 *et seq.,* art. 4; Tallinn Manual 2.0 (note 55), rule 15.

[98] Cf. Draft Articles on State Responsibility (note 97), art. 5; Tallinn Manual 2.0 (note 55), rule 15.

[99] Cf. Draft Articles on State Responsibility (note 97), art. 7; Tallinn Manual 2.0 (note 55), rules 15, commentary, paras. 6, 12.

[100] Cf. Draft Articles on State Responsibility (note 97), art. 16; Tallinn Manual 2.0 (note 55), rule 18 (a).

[101] Cf. Draft Articles on State Responsibility (note 97), art. 16, commentary, para. 1; Tallinn Manual 2.0 (note 55), rule 18, commentary, para. 3.

[102] Cf. Draft Articles on State Responsibility (note 97), art. 8; Tallinn Manual 2.0 (note 55), rule 17 (a).

[103] Cf. UN Group of Governmental Experts, reports of 2013 and 2015 (note 52), paras. 23 and 28 (e) respectively.

[104] Cf. Draft Articles on State Responsibility (note 97), art. 8, commentary, paras. 5 *in fine,* 7.

[105] See also above, 0.

The application of the international rules on State responsibility and hence the act of formally attributing a malicious cyber operation to a State under international law is first and foremost a national prerogative; however, international cooperation and exchange of information with partners in this regard can be of vital importance. In practice, establishing the facts upon which a decision on attribution may be based is of specific concern in the context of cyber operations since the author of a malicious cyber operation may be more difficult to trace than that of a kinetic operation. At the same time, **a sufficient level of confidence** for an attribution of wrongful acts needs to be reached. Gathering relevant information about the incident or campaign in question has a technical dimension and may involve processes of data forensics, open sources research, human intelligence and reliance upon other sources – including, where applicable, information and assessments by independent and credible non-state actors. Generating the necessary contextual knowledge, assessing a suspected actor's motivation for conducting malicious cyber operations and weighing the plausibility of alternative explanations regarding the authorship of a certain malicious cyber act will likewise be part of the process. All relevant information should be considered.[106]

Germany agrees that there is no general obligation under international law as it currently stands to publicize a decision on attribution and to provide or to submit for public scrutiny detailed evidence on which an attribution is based. This generally applies also if response measures are taken.[107] Any such publication in a particular case is generally based on political considerations and does not create legal obligations for the State under international law. Also, it is within the political discretion of a State to decide on the timing of a public act of attribution. Nevertheless, Germany supports the UN Group of Governmental Experts' position in its 2015 report that **accusations of cyber-related misconduct against a State *should* be substantiated**.[108] States should provide information and reasoning and – if circumstances permit – attempt to communicate and cooperate with the State in question to clarify the allegations raised. This may bolster the transparency, legitimacy and general acceptance of decisions on attribution and any response measures taken.[109]

Attribution in the context of State responsibility must be distinguished from politically assigning responsibility for an incident to States or non-State actors: Generally, such statements are made at the discretion of each State and constitute a manifestation of State sovereignty. Acts of politically assigning responsibility may occur in cooperation with partners. As regards attribution in the legal sense, findings of national law-based (court) proceedings involving acts of attribution, for example in the context of criminal liability of certain office holders or non-State actors, may serve as indicators in the process of establishing State responsibility. However, it should be borne in mind that the criteria of attribution under international law do not necessarily correspond to those under domestic law and that additional or specific criteria are generally relevant when establishing State responsibility for individually attributed conduct. Moreover, the adoption of targeted restrictive measures against natural or legal persons, entities or

[106] Cf. also the voluntary, non-binding recommendation made by the UN Group of Governmental Experts, report of 2015 (note 52), para. 13 (b).

[107] On these points, see Tallinn Manual 2.0 (note 55), chapter 4, section 1, para. 13.

[108] UN Group of Governmental Experts, report of 2015 (note 52), para. 28 (f).

[109] Cf. also Tallinn Manual 2.0 (note 55), chapter 4, section 1, para. 13, citing the UN Group of Governmental Experts, report of 2015 (note 52).

bodies under the EU Cyber Sanctions Regime [110] does not as such imply the attribution of conduct to a State by Germany in a legal sense. [111]

b) Measures of response

(1) Retorsion

A State may engage in measures of retorsion to counter a cyber operation carried out against it. Retorsions are unfriendly acts directed against the interests of another State without amounting to an infraction of obligations owed to that State under international law. Since retorsions are predominantly rooted in the political sphere, they are not subject to such stringent legal limitations as other types of response such as countermeasures.

Measures of retorsion may be adopted to **counter (merely) unfriendly cyber operations** perpetrated by another State. They may likewise be enacted in reaction to an unlawful cyber operation **if more intensive types of response (countermeasures, self-defence) are unavailable for legal reasons (for example, in cases in which counter-measures would be disproportionate) or politically unfeasible.** Moreover, they may be adopted as a reaction to an unlawful cyber operation **in combination with other types of response,** such as countermeasures, as part of a State's comprehensive, multi-pronged response to malicious cyber activities directed against it.

(2) Countermeasures

The law of countermeasures allows a State to react, under certain circumstances, to cyber-related breaches of obligations owed to it by another State by taking measures which for their part infringe upon legal obligations it owes to the other State. [112] If certain legal conditions are met, such measures do not constitute wrongful acts under the international law of State responsibility. [113] Germany agrees that **cyber-related as well as non-cyber-related breaches of international obligations may be responded to by both cyber and non-cyber countermeasures**. [114]

As regards the **limitations to countermeasures,** Germany is of the opinion that, **generally, the same conditions apply as in non-cyber-related contexts:** In particular, countermeasures may only be adopted against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations arising from its responsibility (in particular cessation of the wrongful act). [115] Also, they must be proportionate and respect fundamental human rights,

[110] Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I, 17 May 2019, p. 1–12; Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I, 17 May 2019, p. 13–19, as last amended by Council Decision (CFSP) 2020/1748 of 20 November 2020, OJ L 393, 23 November 2020, p. 19-20.

[111] Cf. also Council Decision (CFSP) 2019/797 of 17 May 2019 (note 110), recital 9.

[112] Draft Articles on State Responsibility (note 97), part III, chapter II, introductory commentary; Tallinn Manual 2.0 (note 55), rule 20 (with the commentaries).

[113] Draft Articles on State Responsibility (note 97), art. 22.

[114] Tallinn Manual 2.0 (note 55), rule 20 (with the commentaries).

[115] Draft Articles on State Responsibility (note 97), art. 49 para. 1 (with the commentaries); Tallinn Manual 2.0 (note 55), rule 21.

obligations of a humanitarian character prohibiting reprisals and peremptory norms of international law.[116]

Due to the multifold and close interlinkage of cyber infrastructures not only across different States but also across different institutions and segments of society within States, cyber countermeasures are specifically prone to generating unwanted or even unlawful side effects. Against this background, States must be **particularly thorough and prudent in examining whether or not the applicable limitation criteria to cyber countermeasures are met**.[117]

A State may – *a maiore ad minus* – engage in cyber reconnaissance measures in order to explore options for countermeasures and assess the potential risk of side effects if such measures fulfil the requirements for countermeasures.

(3) Measures taken on the basis of necessity

The wrongfulness of a State's cyber operation that contravenes its international obligations may be precluded by exception if that State acted out of necessity.[118] This entails that a State may – under certain narrow circumstances – act against malicious cyber operations by resorting, for its part, to active counter-operations even in certain situations in which the prerequisites for countermeasures or self-defence are not met.

The draft articles on State responsibility, which reflect customary law in this regard, *inter alia* require that the act must be 'the only way for the State to safeguard an essential interest against a grave and imminent peril'.[119] Whether an 'interest' is 'essential' depends on the circumstances.[120] Germany holds the view that, in the cyber context, the affectedness of an 'essential interest' may *inter alia* be explained by reference to the **type of infrastructure actually or potentially targeted** by a malicious cyber operation and an analysis of that infrastructure's relevance for the State as a whole. For example, the protection of certain critical infrastructures[121] may constitute an 'essential interest'.[122] It might likewise be determined by reference to the ***type* of harm actually or potentially caused** as a consequence of a foreign State's cyber operation. For example, the protection of its citizens against serious physical harm will be an 'essential interest' of each State – regardless of whether a critical

[116] Draft Articles on State Responsibility (note 97), arts. 51, 50 para. 1 (b), (c), and (d); cf. Tallinn Manual 2.0 (note 55), rules 23, 22.

[117] Tallinn Manual 2.0 (note 55), rule 23, commentary, para. 6.

[118] Cf. International Court of Justice (ICJ), Gabčíkovo-Nagymaros Project (Hungary v. Slovakia), Judgement of 25 September 1997, I.C.J. Reports 1997, 7, para. 51; Draft Articles on State Responsibility (note 97), art. 25; Tallinn Manual 2.0 (note 55), rule 26 with commentaries.

[119] Draft Articles on State Responsibility (note 97), art. 25 para. 1 (a). The Draft articles on State Responsibility further require that the act in question must 'not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole' and state that 'necessity may [in any case] not be invoked by a State as a ground for precluding wrongfulness if: (a) the international obligation in question excludes the possibility of invoking necessity; or (b) the State has contributed to the situation of necessity', see art. 25 para. 1 (b) and 2.

[120] Draft Articles on State Responsibility (note 97), art. 25, commentary, para. 15.

[121] On the concept of 'critical infrastructures' see above, 0.

[122] Tallinn Manual 2.0 (note 55), rule 26, commentary, para. 2, correctly noting, however, that the 'designation [of an infrastructure as critical by a State] as such does not necessarily deprive other infrastructure of its essentiality' and that 'a State's unilateral description of infrastructure as critical [is not] determinative of the issue.'

infrastructure is targeted or not. Nevertheless, given the exceptional character of the necessity argument, an 'essential interest' must not be assumed prematurely.

A case-by-case assessment is necessary to determine whether a peril is 'grave'. The more important an 'essential interest' is for the basic functioning of a State, the lower the threshold of the 'gravity' criterion should be. Germany agrees that a **'grave peril' does not presuppose the occurrence of physical injury** but may also be caused by large-scale functional impairments.[123]

A State, when confronted with a cyber threat, **does not yet need to have assessed the *total* and *final* damage potential in order to invoke necessity.**[124] Necessity may be invoked when the origin of a cyber measure has not (yet) been clearly established;[125] however, States should always make efforts to clarify attribution and (State) responsibility in order to be able to substantiate their grounds for action.

(4) Self-defence

The right to self-defence according to art. 51 UN Charter is triggered if an armed attack occurs. Malicious cyber operations can constitute an armed attack whenever they are **comparable to traditional kinetic armed attack in scale and effect.** Germany concurs with the view expressed in rule 71 of the Tallinn Manual 2.0.

Furthermore, Germany acknowledges the view expressed in the ICJ's Nicaragua judgment, namely that an armed attack constitutes the gravest form of use of force.[126] Assessing whether the scale and effects of the cyber operation are grave enough to consider it an armed attack is a political decision taken in the framework of international law. **Physical destruction of property, injury and death (including as an indirect effect) and serious territorial incursions are relevant factors.** The decision is not made based only on technical information, but also after assessing the strategic context and the effect of the cyber operation beyond cyberspace. This decision is not left to the discretion of the State victim of such a malicious cyber operation, but needs to be comprehensibly reported to the international community, i.e. the UN Security Council, according to art. 51 UN Charter.

The response to malicious cyber operations constituting an armed attack is not limited to cyber counter-operations. Once the right to self-defence is triggered, the State under attack **can resort to all necessary and proportionate means in order to end the attack.** Self-defence does not require using the same means as the attack which provided the trigger for its exercise.

---

[123] Tallinn Manual 2.0 (note 55), rule 26, commentary, para. 4.

[124] Cf. Draft Articles on State Responsibility (note 97), art. 25, commentary, para. 16: '[…] a measure of uncertainty about the future does not necessarily disqualify a State from invoking necessity, if the peril is clearly established on the basis of the evidence reasonably available at the time.'

[125] Tallinn Manual 2.0 (note 55), rule 26, commentary, para. 11. Reasonableness standards apply to *ex ante* determinations depending on the context; see also Tallinn Manual 2.0 (note 4), Chapter 4, Introduction to Section 1, para. 9-11.

[126] ICJ, Military and Paramilitary Activities in and against Nicaragua (note 72), para. 191.

Acts of non-State actors can also constitute armed attacks. Germany has expressed this view both with regard to the attacks by Al Qaeda[127] and the attacks of ISIS.[128]

In Germany's view, art. 51 UN Charter requires the attack against which a State can resort to self-defence to be 'imminent'. The same applies with regard to self-defence against malicious cyber operations. Strikes against a prospective attacker who has not yet initiated an attack do not qualify as lawful self-defence.

V. Conclusions and outlook

As has been exemplified in the present paper with regard to a selection of international norms, international law as it stands is capable of providing essential guidance on State behaviour in and with regard to cyberspace. Germany is convinced that **uncertainties as to how international law might be applied in the cyber context can and must be addressed by having recourse to the established methods of interpretation of international law.**[129] Germany deems it critically important that interpretative efforts and attempts to clarify the modalities of the application of international law in cyberspace are based on international exchange and cooperation. This is why Germany follows closely and is actively involved in the work of the **United Nations' working groups on cyber and international security.**[130] In addition to their work on international law in cyberspace, these groups elaborate voluntary, non-binding norms for responsible State behaviour in cyberspace which may fulfil an important function in supplementing the existing 'hard' rules of international law. Moreover, Germany wishes to highlight the importance of States' reflecting and taking heed of the multifold and rich **academic and civil society debates** worldwide on the role and function of international law in the cyber context.

Challenges lie ahead: Information and communication technologies are evolving fast, and so is the need to provide adequate legal assessments and to find responses to novel factual situations. While international law provides a sufficient framework to cope with the fast pace of technological change and remains applicable also to new developments, its interpretation and effective application in the cyber context will increasingly be dependent on an in-depth understanding of technological intricacies and complexities. This may require an **intensified pooling of technical and legal expertise.** Also, evidentiary difficulties with regard to States' and non-State actors' behaviour in cyberspace will continue to pose practical challenges. Nevertheless, while underlining the prime responsibility of States for maintaining peaceful relations and upholding the rule of law in the international system, Germany is convinced that the **combined efforts of States, international organizations, civil society and academia will continue to provide significant insights into the modalities of how international law applies in the cyber context,** thereby leading to a high standard of international legal certainty with regard to this still relatively novel dimension of international relations.

---

[127] See Letter dated 29 November 2001 from the Permanent Representative of Germany to the United Nations addressed to the President of the Security Council, UN Doc. S/2001/1127.

[128] See Letter dated 10 December 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Germany to the United Nations addressed to the President of the Security Council, UN Doc. S/2015/946.

[129] In the case of international treaties, these are codified in arts. 31 *et seq.* of the Vienna Convention on the Law of Treaties, 23 May 1969, UNTS 1155, 331.

[130] I.e. the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) and the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG).

Japan

[Original: English]

1. Status and Purpose

Between 2004 and 2017, five Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), composed of experts appointed by the Secretary-General of the United Nations (UN), were established based on UN General Assembly resolutions. The GGE reports of 2013 and 2015 agreed by consensus by the governmental experts affirm that existing international law, in particular the UN Charter in its entirety, is applicable to cyber operations[131]. By the endorsement of the reports by consensus at the UN General Assembly, this affirmation has become the consensus view of all UN Member States. In the 2015 report, the group offered various important views on how international law applies to cyber operations. The group also recommended continued study on how international law applies. The fifth GGE failed to adopt a report in 2017, one of the reasons for which was that discussions on the application of international law did not achieve a sufficient convergence of opinions. From 2019, the sixth GGE[132] had intensive discussions on how international law applies. Its report was adopted by consensus on May 28, 2021.

This document summarizes the basic position at the moment of the Government of Japan on international law applicable to cyber operations. It was prepared as a national contribution at the request of the Chair of the GGE on the assumption that it will be included in the annex to the group's report to be submitted by the Secretary-General to the General Assembly pursuant to the mandate specified in Resolution 73/266, which requested the Secretary-General to establish the GGE. In this document, the Government of Japan reaffirms that existing international law, including the UN Charter in its entirety, is applicable to cyber operations, and states its present position on how existing international law applies to cyber operations focusing its views on the most important and most basic matters. The contents of this document take into consideration the discussions held by the six GGEs including the current one (governmental experts were appointed from among officials of the Government of Japan to serve on four GGEs, including the current one) and by the Open-ended Working Group (OEWG), which was established in 2019; the discussions held in bilateral and multilateral consultations between the governments of Japan and other States; the results of non-governmental research activities, including Tallinn Manuals 1.0 and 2.0, which were prepared by experts, including those from non-NATO States such as Japan, in their personal capacity with the support of the NATO Cooperative Cyber Defence Centre of Excellence; and the discussions held in multi-stakeholder fora, including ones led by Japan.

The Government of Japan hopes that the announcement of a basic position on international law applicable to cyber operations by the governments of many States and the application of international law in international and domestic courts and tribunals will deepen the shared international understanding on how international law applies to cyber operations. The Government of Japan also hopes that the deepening of a shared understanding—particularly regarding which activities in cyberspace constitute a violation of international law and which tools are available under

[131] In this document, the term "cyber operations" refers to operations using information and communication equipment and technology.

[132] The official name for the sixth GGE is GGE on Advancing responsible State behavior in cyberspace in the context of International Security.

international law for States whose legal interests have been infringed by cyber operations—will deter malicious activities in cyberspace.[133] The Government of Japan's policy is to continue actively participating in relevant discussions, including ones held under the auspices of the UN.

It should be noted that international law applicable to cyber operations is not limited to those mentioned in this document. The Convention on Cybercrime, to which Japan is a party, is an important element of international law applicable to cyber operations. Treaty provisions related to the Data Free Flow with Trust principle, for which Japan is promoting rule-making under the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the Japan-U.S. Digital Trade Agreement, and the Japan-UK Economic Partnership Agreement, also constitute international law applicable to some aspects of cyber operations.

2. International Law Applicable to Cyber Operations

1) Existing international law and the UN Charter

Existing international law, including the UN Charter in its entirety, is applicable to cyber operations.

The 2015 GGE report mentions 11 voluntary, non-binding norms of responsible State behaviour. These items were agreed by Governmental experts as requiring implementation at least as norms, but they include items which affirm or relate to rights and obligations under international law. The inclusion of such norms among the 11 items does not mean that the rights and obligations under existing international law are extinguished or altered.

2) Violation of sovereignty and the principle of non-intervention

A State must not violate the sovereignty of another State by cyber operations. Moreover, a State must not intervene in matters within domestic jurisdiction of another State by cyber operations.

With respect to the principle of non-intervention, cyber operations may constitute unlawful intervention when requirements including the element of coercion, which are clarified in the *Nicaragua* judgement *(1986),*[134] are met.

On the other hand, regarding a violation of sovereignty that does not necessarily constitute an intervention, in the *Lotus* case, the Permanent Court of International Justice held that a State may not exercise its power in the territory of another State,[135] while, in the *Island of Palmas* case, the Arbitral Tribunal stated as follows: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[136] Taking these and other judgments into account, the Government of Japan considers that there exist certain forms of violation of sovereignty which may not necessarily constitute unlawful intervention prohibited under the principle of non-intervention.

---

[133] The term "cyberspace" does not imply the existence of a space which does not belong to real space.

[134] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p.97-98, paragraph 205.

[135] The Lotus case, PCIJ, Series A, No. 10, 1927, p. 18-19.

[136] Island of Palmas Case, Award, RIAA, Vol. II, p. 838.

With respect to violation of sovereignty, the International Court of Justice (ICJ), in the *Nicaragua* case (1986), held that the United States had acted in breach of its obligation under customary international law not to intervene in the affairs of another State, and, in addition, that the United States, by directing or authorizing overflights of Nicaraguan territory, had acted in breach of its obligation under customary international law not to violate the sovereignty of another State.[137] In addition, in the *Costa Rica v. Nicaragua* case (2015), the ICJ cited the absence of evidence that Costa Rica exercised authority on Nicaragua's territory as the reason for dismissing Nicaragua's claim concerning the violation of its territorial integrity and sovereignty.[138] Considering these cases, it can be presumed that, in some cases, a violation of sovereignty constitutes a violation of international law even when it does not fall within the scope of unlawful intervention.

An act of causing physical damage or loss of functionality by means of cyber operations against critical infrastructure, including medical institutions, may constitute an unlawful intervention, depending on the circumstances, and at any rate, it may constitute a violation of sovereignty.[139] As various opinions were expressed on the relationship between violation of sovereignty and unlawful intervention at the sixth GGE and the OEWG, it is desirable that a common understanding be forged through State practices and future discussions.

3) State responsibility

Internationally wrongful acts committed by a State in cyberspace entail State responsibility. An internationally wrongful act occurs when the conduct of a State consisting of an action or omission violates an obligation prescribed by primary rules of international law. In the case of cyber operations as well, there is an internationally wrongful act when a State violates primary rules, including the principles of sovereignty, non-intervention, prohibition of the use of force, as well as various principles of international humanitarian law such as the principle of prohibition of attacks on civilian objects, and respect for basic human rights.

Below, some of the articles of the Articles on Responsibility of States for Internationally Wrongful Acts drafted by the International Law Commission (ILC) (hereinafter referred to as the "ILC's Articles on State Responsibility") are mentioned as a reference. However, it should be noted that the Articles have not been adopted as a treaty text and the question of whether or not each article reflects customary international law has to be closely examined.

a) Attribution

There is an internationally wrongful act of a State when the act is attributable to the State under international law and when the act constitutes a breach of an obligation of the State under international law.

There are legal, political and technical aspects in discussing the attribution of conduct to a State with respect to cyber operations.

---

[137] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p.136-139, paragraph 292.

[138] Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Judgment, I.C.J. Reports 2015, p. 738, paragraph 223.

[139] Tallinn Manual 2.0 also mentions physical damage to or loss of functionality of cyber infrastructure as a case that may constitute violation of sovereignty.

To invoke State responsibility under international law with respect to any act in cyberspace, it is necessary to consider whether the act is attributable to a specific State. On this topic, Articles 4 to 11 of the ILC's Articles on State Responsibility provide useful reference. As a general rule, in such cases as a cyber operation conducted by a State organ, the act is considered to be attributable to the State. A cyber operation conducted by a non-State actor is, in principle, not attributable to a State. However, according to Article 8 of the ILC's Articles on State Responsibility, the conduct of a person or group of persons shall be considered an act of a State if the person or group of persons is in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct.[140]

b) Obligations of a State responsible for an internationally wrongful act

Regarding cyber operations as well, a State responsible for an internationally wrongful act is under the following obligations. First, the State shall cease the act if it is continuing. In addition, the State shall offer appropriate assurances and guarantees of non-repetition, if circumstances so require. Besides, the responsible State is under an obligation to make full reparation for the injury caused by the internationally wrongful act.

c) Countermeasures and necessity

Under international law, it is permitted, under certain conditions, to take countermeasures against internationally wrongful acts.

In general terms, under international law, a State which has been injured by an internationally wrongful act of another State may take, under certain conditions, countermeasures in order to induce the responsible State to comply with (i) the obligation to cease the international wrongful act and (ii) the obligation to make reparation.

General international law does not confine countermeasures to those with the same means as the preceding internationally wrongful act in response to which they are taken. Japan considers that this is the same for the countermeasures against internationally wrongful acts in cyberspace.

The Government of Japan is of the view that a State may invoke necessity under international law when the requirements shown in Article 25 of the ILC's Articles on State Responsibility are satisfied.

4) Due diligence

States have a due diligence obligation regarding cyber operations under international law. Norm 13(c) and (f) and the second half of paragraph 28(e) of the 2015 GGE report are related to this obligation.

In the *Corfu Channel* case (1949), the ICJ referred to the existence of "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".[141] In relation to cyber operations, the due diligence obligation in this sense has significance.

Furthermore, with regard to the concept of the due diligence obligation, the Alabama Arbitral Award (1872) held that "due diligence" ought to be exercised by neutral governments in exact proportion to the risks to which either of the belligerents

[140] Article 8 of the ILC's Articles on State Responsibility

[141] Corfu Channel case, Judgment of April 9th, 1949: I.C.J. Reports 1949, P.22.

may be exposed, from a failure to fulfil the obligations of neutrality on their part,[142] and, in the *Genocide Convention (Bosnia and Herzegovina v. Serbia and Montenegro)* case (2007), the ICJ seems to consider the nature of the obligation to prevent genocide under the Genocide Convention to be the due diligence obligation and referred to an obligation of the contracting States to exercise the capacity to influence the actions of persons likely to commit genocide to prevent genocide so far as possible.[143]

The outer limit of the due diligence obligation of territorial States with respect to cyber operations is not necessarily clear. By reference to these judgements related to the concept of the due diligence obligation, it seems necessary to consider on a case-by-case-basis the scope of the obligation taking into account such factors as the seriousness of the cyber operations in question and the capacity of the territorial States to influence a person or group of persons conducting the attacks.

In light of the above, at the least, for example, when a State has received a credible notification from another State of the possibility that a person or group of persons located in its territory and receiving from it financial and other forms of support may be involved in a cyber operation that may cause serious adverse consequences, such as damage to a target State's critical infrastructure, the due diligence obligation owed by the informed State is presumed to include the obligation to exercise its capacity to influence the state-supported person or group of persons so as to prevent them from implementing such cyber operations.

One characteristic of cyber operations is the difficulty of making judgment as to attribution to a State. In this respect, the due diligence obligation may provide grounds for invoking the responsibility of the State from the territory of which a cyber operation not attributable to any State originated. It is possible at least to invoke the responsibility of such a State for a breach of its due diligence obligation, even if it is difficult to prove the attribution of a cyber operation to any State.

5) Peaceful settlement of disputes, prohibition of the use of force, and the right to self-defense

a) Peaceful settlement of disputes

Any international disputes involving cyber operations must be settled through peaceful means pursuant to Article 2(3) of the UN Charter. In addition, pursuant to Article 33 of the UN Charter, the parties to any dispute involving cyber operations, the continuance of which is likely to endanger the maintenance of international peace and security, must first of all seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice. In order to ensure the peaceful settlement of disputes, the powers of the Security Council based on Chapters VI and VII of the UN Charter and the functions of the other UN organs, including ICJ based on Chapter XIV of the UN Charter and the Statute of the International Court of Justice should be used in disputes stemming from cyber operations.

b) Prohibition of the use of force

Under certain circumstances, a cyber operation may constitute the threat or use of force prohibited by Article 2(4) of the UN Charter. Pursuant to this article, all States shall refrain in their international relations from the threat or use of force. The

[142] Alabama claims of the United States of America against Great Britain, RIAA, Vol XXIX, p.129

[143] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 221, paragraph 430.

Government of Japan presumes that as a general rule the threat of force refers to a State's act of threatening another State by indicating its intention or attitude of using force, without actually using force, unless its arguments or demands are accepted. The obligation to refrain from the threat or use of force in international relations is an important obligation relating to cyber operations.

c) Right of self-defense

When a cyber operation constitutes an armed attack under Article 51 of the UN Charter, States may exercise the inherent right of individual or collective self-defense recognized under Article 51 of the UN Charter.

6) International humanitarian law

International humanitarian law is also applicable to cyber operations.

In situations of armed conflict, the methods and means of warfare used by the parties to the conflict are subject to regulations under international humanitarian law. This extends to cyber operations implemented by the parties to the conflict. Several principles under international humanitarian law, including the principle of humanity, necessity, proportionality and distinction, are also applicable to acts in cyberspace. In paragraph 28(d) of the 2015 GGE report, those principles are referred to as "established international legal principles." This reference, considered together with the fact that this report affirms the applicability of existing international law, can be interpreted to affirm the applicability of those principles. Meanwhile, Article 49 of the Additional Protocol I to the Geneva Conventions stipulates: "'Attacks' means acts of violence against the adversary, whether in offence or in defence."[144,145] The Government of Japan understands that cyber operations that may cause the destruction or neutralization of military targets, for example, may also constitute "attacks" under international humanitarian law, depending on the circumstances.

In principle, the existence of an "armed conflict" is a prerequisite for the application of international humanitarian law. Under the Geneva Conventions, there is no particular definition of an "armed conflict," and therefore, whether or not a certain incident constitutes an "armed conflict" needs to be decided on a case-by-case basis, taking into account a number of elements, such as the manner of the actual attack and the intent of each party to the incident, in a comprehensive manner. If the effects of cyber operations are taken into consideration, the conduct of cyber operations alone may reach the threshold of an "armed conflict."

As affirming the applicability of international humanitarian law to cyber operations contributes to the regulation of methods and means of warfare, the argument that doing so will lead to the militarization of cyberspace is groundless. For example, cyber operations during armed conflict that cause physical damage or loss of functionality to medical institutions may constitute a violation of international humanitarian law[146] and therefore should be appropriately regulated. On the other hand, modes of combat in cyberspace are different from those in traditional domains.

---

[144] "Attacks" means acts of violence against the adversary, whether in offence or in defense (Article 49 of the Additional Protocol I to the Geneva Conventions).

[145] Tallinn Manual 2.0 stipulates that "a cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." (Tallinn Manual 2.0., Rule 92).

[146] For example, Article 12 of the Additional Protocol I to the Geneva Conventions.

Therefore, how international humanitarian law regarding, for example, the scope of combatants applies to cyberspace should be further discussed.

7) International human rights law

International human rights law is also applicable to cyber operations. Individuals enjoy the same human rights with respect to cyber operations that they otherwise enjoy. Pursuant to international human rights law, States are under the obligation to respect human rights. The human rights that must be respected in cyberspace include all human rights that are recognized under international human rights law, such as civil, political, economic, social and cultural rights. The human rights that are particularly relevant in the context of cyberspace include the right to privacy, freedom of thought and conscience, freedom of expression, and guarantee of due process. The final sentence of paragraph 28(b) of the 2015 GGE report affirms the above. While Norm 13(e) of the report affirms some of the obligations under international human rights law, it does not change the obligations that are not mentioned therein.

Kazakhstan

[Original: Russian]

Международные документы в сфере использования информационно-коммуникационных технологий

Большинство фундаментальных международных документов в области защиты прав человека, такие как Конвенция Совета Европы о защите прав человека и основных свобод от 1950 года, Международный пакт Организации Объединенных Наций (далее – Международный пакт ООН) о гражданских и политических правах от 1966 года признают в качестве одного из основных прав человека право на свободу поиска, получение и распространение всякого рода информации и идей, независимо от государственных границ, основываясь на праве невмешательства в личную жизнь.

Пользование вышеуказанными правами налагает особые обязанности и особую ответственность. Оно может быть, следовательно, сопряжено с некоторыми ограничениями, которые, однако, должны быть установлены законом и являться необходимыми уважения прав и репутации других лиц и охраны государственной безопасности, общественного порядка, здоровья или нравственности населения (п.3 ст.19 Международного пакта ООН).

В соответствии со статьей 20 Международного пакта ООН всякая пропаганда войны должна быть запрещена законом. Всякое выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию, должно быть запрещено законом.

Применимость международного права в Казахстане

В целом данные нормы Международного пакта ООН применяются в Казахстане.

К примеру, согласно статье 1 Закона Республики Казахстан «О противодействии экстремизму» разжигание расовой, национальной и родовой розни, религиозной вражды или розни, а также применение любой религиозной практики, вызывающей угрозу безопасности, жизни, здоровью, нравственности или правам и свободам граждан является экстремизмом.

На территории Республики Казахстан запрещаются использование сетей и средств связи для осуществления экстремизма, а также ввоз, издание, изготовление и (или) распространение экстремистских и террористических материалов (ст.12 Закона «О противодействии экстремизму» и ст.10-4 Закона «О противодействии терроризму»).

Кроме того, в Казахстане действует Закон «О персональных данных и их защите» (от 21.05.2013г.), что соответствует к требованию пункта 1 статьи 4 Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (от 1981 года), где указано, что каждая сторона принимает необходимые меры в рамках своего внутреннего законодательства в целях придания юридической силы основополагающим принципам защиты персональных данных.

Целью настоящего Закона является обеспечение защиты прав и свобод человека и гражданина при сборе и обработке его персональных данных.

Также одним из важнейших документов, регулирующих правоотношения в сфере глобальной компьютерной сети, является Конвенция Совета Европы о киберпреступности, принятая в ноябре 2001 года в Будапеште.

Казахстаном также применяются нормы указанной Конвенции.

В частности, согласно статьям 2-11 Конвенции Совета Европы о киберпреступности (противозаконный доступ к компьютерной системе, неправомерный перехват не предназначенных для общего пользования компьютерных данных, умышленное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных, умышленное создание неправомерно серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, 3 изменения или блокирования компьютерных данных, противозаконное использование устройств, подлог с использованием компьютерных технологий, мошенничество с использованием компьютерных технологий, правонарушения, связанные с детской порнографией, правонарушения, связанные с нарушением авторского права и смежных прав, покушение, соучастие или подстрекательство к совершению вышеуказанных преступлений) каждая сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать действия, связанные с противоправным использованием компьютерных систем в качестве уголовного преступления. Данные нормы отражены в седьмой главе (уголовные правонарушения в сфере информатизации и связи, ст.205-213 УК), а также в статьях 190 (мошенничество), 369 (служебный подлог), 312 (изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних либо их привлечение для участия в зрелищных мероприятиях порнографического характера) и 198 (нарушение авторских и (или) смежных прав) Уголовного кодекса Республики Казахстан.

Уголовно-процессуальный кодекс Республики Казахстан (Глава 7, далее – УПК РК) регламентирует процедуру международного сотрудничества в сфере уголовного судопроизводства, отраженные в Конвенции Совета Европы о киберпреступности.

Кроме того, в 1990 году VIII Конгресс ООН по предупреждению преступности и обращению с правонарушителями принял резолюцию, призывающую государства – члены ООН увеличить усилия по борьбе с компьютерной преступностью, модернизируя национальное уголовное законодательство, содействовать развитию в будущем структуры международных принципов и стандартов предотвращения, судебного преследования и наказания в области компьютерной преступности. 14 декабря 1990 года Генеральной Ассамблеей ООН была принята резолюция, призывающая правительства государств-членов руководствоваться решениями, принятыми на VIII Конгрессе ООН.

Kenya

[Original: English]

How International Law Applies to the Use of Information and Communication Technologies by States

For more than half a century, information and communication technology (ICT) has been international in its creation, reach, use and misuse. Therefore, States have recognized the need to create effective and sustainable frameworks to guide the use of ICTs in the context of international security.

The applicability of International Law towards this effort was first formally stated in Article 19 of the 2013 of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) which states that "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment." The 2015 report of the same group went further in Article 25 and emphasized the role of International law as an essential framework for actions in the use of ICTs. As a member of the UNGGE since 2014, and the United Nations General Assembly (UNGA) that has consistently endorsed the reports presented through the UN Secretary General and recommended that States should implement the recommendations of each report, the Republic of Kenya concurs that international law provides critical guidance for the use of ICTs.

Kenya recognizes that, although the existing International Law does not include an explicit reference to the use of ICTs in the context of international security, nevertheless, negative trends in the digital domain continue to undermine state, regional and international security and stability. This reality requires States to commit to address these threats through a common understanding of how the existing agreed frameworks, including International Law, apply, to ensure an open, secure, stable, accessible and peaceful global ICT environment. In this regard, it is evident that additional efforts should be made to build capacity in International Law and effective national ICT legislation to enable States to develop their own understanding of how International Law applies to the use of ICTs within their specific contexts. Further exchange of views between States will contribute to the development of workable norms and rules to address specific scenarios and discourage behaviour that is in violation of the principles of International Law.

Due to the exponential nature of advancements of ICTs, it is critical to have an evolving shared understanding of the threats posed by the use of ICTs in matters related to regional and international peace and security. The international community should support efforts by States to address these threats through the framework of state sovereignty, international law, voluntary norms and confidence-building measures.

Kenya acknowledges the important contribution of International Law in national governance. The Constitution of Kenya 2010 Article 2(5) states that "the general rules of International Law shall form part of the Law of Kenya." Kenya recognizes that International Law has many functions. Among the primary functions is to create an agreed context and standard of action and behaviour among States, to maintain order in international issues, to minimize the occurrence of international conflicts and disputes, and, where they occur, to assist in their resolution, and lastly, to protect the sovereign liberties and rights of States. The basic rights of States must include the ability to dwell in peace, to develop and to prosper. While National laws may focus on the interests of the Individual State, International law should be implemented in order to promote the well-being of all States and all people and to protect them from harm.

It is clear that in the modern world applications of ICTs cross borders. The most obvious example is the operation of the Internet where both the technology and its application assume participation by many stakeholders domiciled in different States. The Internet, while locally managed and experienced is truly an international infrastructure. However, there are many other applications of ICTs that cross borders: social media platforms, ecommerce systems, e-learning environments, enterprise systems operated by multinational companies among others. With the operation of the Internet as well as other global internetworks, Cybersecurity has become a major concern between States since breaches of network security can almost instantaneously move from one State to another. Therefore, States recognize that, while the internal management of ICTs by States is imperative, it is also important for States to work together to promote law, methodology and practice that spans borders.

Kenya has developed Policy, Legal and Institutional Frameworks to ensure the maintenance of a secure ICT environment. On the Legal framework, Kenya has enacted the Computer Misuse and Cybercrimes Act 2018 and the Data Protection Act 2019 and is currently developing the Critical Infrastructure Bill. On Institutional framework, Kenya has established Institutions devoted to information security such as KE-CERT, and the National Cyber Command Centre as well as the ICT Authority which carries out capacity building and cyber-hygiene activities and gives operational guidance at times of special need (for example when a large number of persons and organizations moved to use ICTs for teleconferencing to mitigate the impact of the COVID-19 pandemic).

In recognition of the importance of regional and international policy-making Kenya has participated in such various fora where ICT in the context of International Security has been discussed, such as the East African Community, the Northern Corridor Forum, the African Union the UN Open-ended Working Group (OEWG) and the UNGGE.

The UN Charter forms a strong foundation for the interpretation of existing international laws underlined by inter alia the principles of State sovereignty, sovereign equality, and settlement of international disputes by peaceful means. It is the Charter's emphasis on these principles that is fully aligned with Kenya's peaceful stance in international affairs. Kenya notes that there is a strong body of International Law which can be applied in the context of ICTs including Human Rights Law based on the Universal Declaration of Human Rights, International Humanitarian Law (recognizing that, unfortunately, not only can ICTs become a source of conflict, but they are increasingly both used and developed during conflicts between States) and Customary International Law. All these laws should be studied and analyzed in a fair, open, peace-loving and balanced manner in order to adopt a utilitarian body of International Law that guides the use of information and communication technology in the context of international security.

As States study International Law through National, Regional and International processes, it is important to consider how these laws will be effectively applied in future. The mechanisms, institutions and capacity must be built to carry the agreed laws and frameworks from the boardroom to the working environment. Kenya remains committed to the process of analyzing, negotiating, agreeing and operationalizing International Law in order to advance responsible State behavior in cyberspace in the context of international security.

Netherlands

[Original: English]

Introduction

In this appendix the government will discuss a number of significant obligations under international law that apply to states in cyberspace. Any violation of these obligations that is attributable to a state constitutes an internationally wrongful act, unless there is a ground for precluding the wrongfulness of an act recognised in international law.[147]

As the government has indicated on multiple occasions and consistently argues, international law is applicable in cyberspace. This is also recognised internationally.[148] Nevertheless, there are still many unanswered questions concerning the precise manner in which international law should be applied in cyberspace. This is due to the unique characteristics of the digital world in comparison with the physical world. Digital data generally moves rapidly and is therefore often difficult to localise. It can be transferred to another country in a matter of seconds, and can be stored across a range of different countries. What is more, undesirable activity in cyberspace does not necessarily always have an immediate physical impact, even though its effects may nonetheless be serious. It is not yet entirely clear how these and other unique characteristics should be dealt with in the application of international law. The government is encouraging international debate on ways to clarify the application of international law in cyberspace. Clarity and consensus on these points are essential to the international legal order.

The formulation of responses to these questions is an ongoing process, in which the government coordinates closely with like-minded partners and pursues initiatives aimed at furthering dialogue, such as the international consultations on international law in cyberspace hosted by the Netherlands in The Hague in late May 2019.

In this appendix the government will discuss a number of significant rules of international law that apply to states in cyberspace. It also explains its interpretation of the application of those rules. Where relevant, it indicates what issues are still the subject of international debate and need to be elaborated further. The following topics will be considered in turn: the obligations of states in cyberspace, the attribution of cyber operations, and options for responding to undesirable cyber activity by another state. The government has taken the primary sources of international law defined in article 38 of the Statute of the International Court of Justice as a starting point. This article refers,*inter alia*, to international conventions, international custom and the general principles of law as sources of international law.

[147] The responsibility of states and the grounds for precluding the wrongfulness of an act under international law are laid down, *inter alia,* in the Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA), which is included in UN General Assembly resolution A/56/589. The commentary on the ARSIWA is included in the *Yearbook of the International Law Commission*, 2001, vol. II, Part Two.

[148] See, for example, the 2013 and 2015 reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: https://www.un.org/disarmament/ict-security/; EU Cybersecurity Strategy, 2017; NATO Summit Declarations of 2014, 2016 and 2018.

Obligations of states

Respect for sovereignty

The principle of sovereignty, i.e. that states are equal and independent and hold the highest authority within their own borders, is one of the fundamental principles of international law.[149] More specific rules of international law, such as the prohibition of the use of force, the principle of non-intervention and the right of self-defence stem from this principle. These rules will be discussed in more detail below.

According to some countries and legal scholars, the sovereignty principle does not constitute an independently binding rule of international law that is separate from the other rules derived from it. The Netherlands does not share this view. It believes that respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act. This view is supported, for example, by the case law of the International Court of Justice, which ruled in Nicaragua v. United States of America that the United States had acted in breach of its obligation under customary international law not to violate the sovereignty of another state.[150] Below the government will discuss the significance of this obligation in more detail.

Firstly, sovereignty implies that states have exclusive jurisdiction over all persons, property and events within their territory, within the limits of their obligations under international law, such as those relating to diplomatic privileges and immunity, and those arising from human rights conventions. This is the internal aspect of sovereignty. Secondly, sovereignty implies that states may freely and independently determine their own foreign policy, enter into international obligationsand relations, and carry out activities beyond their own borders, provided they respect the rules of international law. This is the external aspect of sovereignty.

Both aspects apply equally in cyberspace. States have exclusive authority over the physical, humanand immaterial (logical or software-related) aspects of cyberspace within their territory. Within their territory they may, for example, set rules concerning the technical specifications of mobile networks, cybersecurity and resilience against cyberattacks, take measures to combat cybercrime, and enforcethe law with a view to protecting the confidentiality of personal data. In addition, they may independently pursue foreign ‘cyber’ policy and enter into treaty obligations in the area of cybersecurity. The Netherlands’ decision to accede to the Convention on Cybercrime of the Council of Europe is an example of the exercise of Dutch sovereignty.

States have an obligation to respect the sovereignty of other states and to refrain from activities that constitute a violation of other countries’ sovereignty. Equally, countries may not conduct cyberoperations that violate the sovereignty of another country. It should be noted in this regard that theprecise boundaries of what is and is not permissible have yet to fully crystallise. This is due to the firmly territorial and physical connotations of the traditional concept of sovereignty. The principle has traditionally been aimed at protecting a state's authority over *property and persons within its own national borders.* In cyberspace, the concepts of territoriality and physical tangibility are often less clear. It is possible, for example, for a single cyber

[149] *Island of Palmas arbitral award of 1928:* ‘Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.’

[150] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), International Court of Justice (ICJ), 27 June 1986, paras 15 and 292.

operation to be made up of numerous components or activities initiated from or deployed via different countries in a way that cannot always be traced. In addition, there are various ways of masking the geographic origin of activitiesperformed in cyberspace. What is more, data stored using a cloud-based system is often moved from one location to another, and those locations are not always traceable. So it is by no means always possible to establish whether a cyber operation involves a cross-border component and thusviolates a country's sovereignty. Even if the origin or route of a cyber operation can be established, these kinds of operations do not always have a direct physical or tangible impact.

From the perspective of law enforcement (which is part of a state's internal sovereignty), the manner in which the principle of sovereignty should be applied has not fully crystallised at international level either. Shared investigative practices do seem to be developing in Europe and around the world, however. Data relevant to criminal investigations is increasingly stored beyond national borders, for example in the cloud, in mainly private data centres. And when it comes to criminal offences committed on, or by means of, the internet, the location of data – including malicious software or code – and physical infrastructure is often largely irrelevant. It is easy to hide one's identity and location on the internet, moreover, and more and more communications are now encrypted. Even in purely domestic criminal cases – including cybercrime – where the suspect and victim are both in the Netherlands, cyber investigations often encounter data stored beyond our borders, particularly when investigators require access to data held by online service providers or hosting services, or need to search networks or (covertly) gain remote entry to an automated system. The act of exercising investigative powers in a cross-border context is traditionally deemed a violation of a country's sovereignty unless the country in question has explicitly granted permission (by means of a treaty or other instrument). Opinion is divided as to what qualifies as exercising investigative powers in a cross-border context and when it is permissible without a legal basis founded in a treaty. In cyberspace too, countries' practices differ in their practical approaches to the principle of sovereignty in relation to criminal investigations. The Netherlands actively participates in international consultations on the scope for making investigations more effective, paying specific attention to ensuring the right safeguards are in place. In general the government endorses Rule 4, proposed by the drafters of the Tallinn Manual 2.0, on establishing the boundaries of sovereignty in cyberspace.[151] Under this rule, a violation of sovereignty is deemed to occur if there is 1) infringement upon the target State's territorial integrity; and 2) there has been an interference with or usurpation of inherently governmental functions of another state. The precise interpretation of these factors is a matter of debate.

Non-intervention principle

The development of advanced digital technologies has given states more opportunities to exert influence outside their own borders and to interfere in the affairs of other states. Attempts to influence election outcomes via social media are an example of this phenomenon. International lawsets boundaries on this kind of activity by means of the non-intervention principle, which is derived from the principle of sovereignty. The non-intervention principle, like the sovereignty principle fromwhich it stems, applies only between states.

Intervention is defined as interference in the internal or external affairs of another state with a view to employing coercion against that state. Such affairs concern

[151] The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* was drafted by a team of experts on international law in consultation with governmental legal practitioners.

matters over which, in accordance with the principle of sovereignty, states themselves have exclusive authority. National elections are an example of internal affairs. The recognition of states and membership of international organisations are examples of external affairs.

The precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallisedin international law. In essence it means compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue. The goal of the intervention must be to effect change in the behaviour of the target state. Although there is no clear definition of the element of coercion, it should be noted that the use of force will always meet the definition of coercion. Use of force against another state is always a form of intervention.

Prohibition of the use of force

Article 2(4) of the UN Charter lays down a prohibition on the threat or use of force. It reads as follows: 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state.' This prohibition applies to the use of force in any form, regardless of the weapons or means employed.[152]

The prohibition of the use of force is virtually absolute. There are only three situations in which the threat or use of force does not contravene international law. One is in the case of self-defence against an armed attack (article 51 of the UN Charter). Another concerns certain actions implementing a UN Security Council resolution under Chapter 7 of the Charter.[153] The final exception is when the use of force takes place with the agreement of the state in whose territory that force will be used.

When applying this prohibition in the context of cyberspace, the question arises: when can cyber operations be considered 'use of force', given that no use is made of 'weapons' in the usual (physical) sense of the word? The government believes that cyber operations can fall within the scope of the prohibition of the use of force, particularly when the effects of the operation are comparable to those of a conventional act of violence covered by the prohibition. In other words, the effects of the operation determine whether the prohibition applies, not the manner in which those effects are achieved. This position is supported by the case law of the International Court of Justice, which has ruled that the scale and effects of an operation must be considered when assessing whether an armed attack in the context of the right of self-defence has taken place (see below). There is no reason not to take the same approach when assessing whether an act may be deemed a use of force within the meaning of article 2 (4) of the UN Charter. A cyber operation would therefore in any case be qualified as a use of force if its scale and effects reached the same level as those of the use of force in non-cyber operations.

International law does not provide a clear definition of 'use of force'. The government endorses the generally accepted position that each case must be examined individually to establish whether the 'scale and effects' are such that an operation may be deemed a violation of the prohibition of use of force. In their 2011 advisory report 'Cyber Warfare', the Advisory Council on International Affairs (AIV) and the Advisory Committee on Issues of Public International Law (CAVV) noted that, 'The

[152] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, International Court of Justice (ICJ), 8 July 1996, para. 39.

[153] In international law the use of force is not the same as an armed attack. The latter term is relevant in the context of the right of self-defence. This will be discussed further on page 69.

customary interpretation of this provision is that all forms of armed force are prohibited. Purely economic, diplomatic and political pressure or coercion is not defined as force under article 2, paragraph 4. Suspending trade relations or freezing assets, for example, can be very disadvantageous to the state affected but has not to date been considered a prohibited form of force within the meaning of the Charter. Armed force that has a real or potential physical impact on the target state is prohibited.'[154] In the view of the government, at this time it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force.

It is necessary, when assessing the scale and effects of a cyber operation, to examine both qualitative and quantitative factors. The Tallinn Manual 2.0 refers to a number of factors that could play a role in this regard, including how serious and far-reaching the cyber operation's consequences are, whether the operation is military in nature and whether it is carried out by a state.[155] These are not binding legal criteria. They are factors that could provide an indication that a cyber operation may be deemed a use of force, and the government endorses this approach. It should be noted in this regard that a cyber operation that falls below the threshold of use of force may nonetheless be qualified as a prohibited intervention or a violation of sovereignty.

The due diligence principle

The due diligence principle holds that states are expected to take account of other states' rights when exercising their own sovereignty. The principle is articulated by the International Court of Justice, for example, in its judgment in the Corfu Channel Case,[156] in which it held that states have an obligation to act if they are aware or become aware that their territory is being used for acts contrary to the rights of another state. It should be noted that not all countries agree that the due diligence principle constitutes an obligation in its own right under international law. The Netherlands, however, does regard the principle as an obligation in its own right, the violation of which may constitute an internationally wrongful act.

In the context of cyberspace, the due diligence principle requires that states take action in respectof cyber activities:

– carried out by persons in their territory or where use is made of items or networks thatare in their territory or which they otherwise control;

– that violate a right of another state; and

– whose existence they are, or should be, aware of.[157]

To this end a state must take measures which, in the given circumstances, may be expected of a state acting in a reasonable manner. It is not relevant whether the

[154] 'Cyber Warfare', Advisory report no 77, AIV/no. 22, CAVV December 2011, p. 20.

[155] Tallinn Manual 2.0, Rule 69.

[156] Corfu Channel Case; Assessment of Compensation (United Kingdom v. Albania), International Court of Justice (ICJ), 9 April 1949, para. 22.

[157] *Corfu Channel Case; Assessment of Compensation (United Kingdom v. Albania)*, International Court of Justice (ICJ), 9 April 1949, para 44. The International Court of Justice concluded that the constructive knowledge standard of the due diligence principle (within the meaning of international law) is also met if a state should have known that the activity in question took place on its territory. Specifically this means that a state has an obligation to do everything feasible. Precisely what constitutes fulfilment of this requirement in the context of cyberspace is currently still a matter of debate.

cyber activity in question is carried out by a state or non-state actor, or where this actor is located. If, for example, a cyberattackis carried out against the Netherlands using servers in another country, the Netherlands may, on the basis of the due diligence principle, ask the other country to shut down the servers, regardless of whether or not it has been established that a state is responsible for the cyberattack.

It is generally accepted that the due diligence principle applies only if the state whose right or rights have been violated suffers sufficiently serious adverse consequences. The precise threshold dependson the specific circumstances of the case. It is clear, however, that such adverse consequences do not necessarily have to include physical damage.

Obligations relating to armed conflict – international humanitarian law

International humanitarian law (IHL) applies to actions in the context of armed conflict. This includes cyber operations carried out as part of an armed conflict. The existence of an armed conflict (international or non-international) is thus a requirement for the application of this specialised area of law. As early as 2011, the government observed that applying the rules of international humanitarian law (jus in bello) to hostilities in cyberspace is 'technically feasible and legally necessary'.[158]

A key component of IHL is international law on neutrality. Neutrality requires that states which are not party to an armed conflict refrain from any act from which involvement in the conflict may be inferred or acts that could be deemed in favour of a party to the conflict. In its relations with parties to the armed conflict the neutral state is required to treat all parties equally in order to maintain its neutrality. A state may not, for example, deny access to its IT systems to one party to the conflict but not to the other. In its response to the above-mentioned advisory report by the AIV/CAVV, the government noted that, 'In an armed conflict involving other parties, the Netherlands can protect its neutrality by impeding the use by such parties of infrastructure and systems (e.g. botnets) on Dutch territory. Constant vigilance, as well as sound intelligence and a permanent scanning capability, are required here.'[159]

IHL also lays down specific rules regarding attacks aimed at persons or objects, which apply equally to cyber operations carried out as part of an armed conflict.[160] When planning and carrying out such operations, states must act in accordance with, for example, the principles of distinction and proportionality, as well as the obligation to take precautionary measures.

Human rights

Human rights are an important component of international law which are laid down in a number of instruments, such as UN treaties and the European Convention on Human Rights (ECHR). Human rights include the right to life, the prohibition of torture and inhuman or degrading treatment, and the right to a fair trial.

States have a duty to respect and protect the human rights of every person within their jurisdiction.This implies not only a 'negative' duty – i.e. to refrain from acts in

[158] 'Cyber Warfare', Advisory report no 77, AIV/no. 22, CAVV December 2011, p. 25; government response to the AIV/CAVV report 'Cyber Warfare', 17 January 2012.

[159] 'Cyber Warfare', Advisory report no 77, AIV/no. 22, CAVV December 2011, p. 26.

[160] Additional Protocol to the Geneva Conventions of 12 August 1949 relating to International Armed Conflicts (Protocol I), Bern, 8 June 1977, article 49; *Tallinn Manual 2.0*, Rule 92. It is beyond the scope of this letter to consider the technical debate on the difference between a cyber operation and a cyberattack in the context of an armed conflict.

violation of human rights – but also a 'positive' duty to ensure that people can genuinely exercise their rights and defend themselves against violations by others. It is for instance not sufficient for the Dutch government to respect theprivacy of Dutch citizens. It must also take measures to ensure that, for example, companies respect the privacy of their customers.

Most human rights are not absolute. This means that some restriction of rights is permissible undercertain circumstances. For example, states may criminalise hate speech or incitement to violence, even though doing so has implications for certain individuals in terms of their freedom of expression.The assessment of whether a given restriction is justified depends on the treaty provision concerned.In most cases, however, the factors to be weighed include whether the restriction serves a legitimate purpose, has a valid legal basis and is necessary and proportionate. In addition, in an emergency situation, the observance of a limited number of human rights may be partly suspended for a limitedperiod. One example is the introduction of a curfew when in a state of war.

Human rights are just as valid in cyberspace as they are in the physical domain. There is no difference between online and offline rights. This has been recognised by the United Nations General Assembly, among others.[161]However, it is clear that ongoing digitalisation and technological advances are raising new questions and presenting new challenges when it comes to the applicationof human rights. The increased scope for collecting, storing and processing data creates issues concerning the right to privacy. Similarly, the increased options for people to express their views viaonline platforms raise questions with regard to the freedom of expression. It is conceivable that in the future a number of these issues will require further regulation at national or international level.At present, however, the government believes that the existing range of human rights instrumentsprovides sufficient scope for effectively safeguarding the protection of human rights in cyberspace.

It is also clear that access to the internet is becoming increasingly important to the effective exercise of human rights, not only for human rights defenders and NGOs (which can use social media to drawattention to human rights violations and mobilise support), but for everyone. Rights such as freedom of expression and freedom of association and assembly have gained a new dimension with the adventof social media, as have the right to education and the right to health, given the wealth of informationand training courses available online. The right to privacy and the right to family life are another example, thanks to the increased scope for digital communication. At the same time the risk of violations of human rights online has also increased. There is now more scope for surveillance, and disinformation has become more widespread.

The growing relevance of the internet to human rights underlines the need for a secure, open andfree internet. The government is working at international level to promote this aim.

Attribution

For a state to be held responsible under international law for a cyber operation and, by extension, for a target state to be able to take a countermeasure in response,[162] it must be possible to attribute the operation to the state in question. Any attribution of cyber operations is always based on a government decision. Special attention is

[161] See e.g. 'The Right to Privacy in the Digital Age', General Assembly Res. 68/167, para. 3, UN Doc. A/RES/68/167 (December 2013).

[162] For a discussion of countermeasures see page 62 of this appendix.

paid to the degree to which the government has information of its own at its disposal or to which it is able to reach an independent conclusion concerning information it has obtained.

In the context of cyberspace, three forms of attribution can be distinguished:

– Technical attribution – a factual and technical investigation into the possible perpetrators ofa cyber operation and the degree of certainty with which their identity can be established.

– Political attribution – a policy consideration whereby the decision is made to attribute (publicly or otherwise) a specific cyber operation to an actor without necessarily attaching legal consequences to the decision (such as taking countermeasures). The attribution need not necessarily relate to a state; it may also concern a private actor.

– Legal attribution – a decision whereby the victim state attributes an act or omission to a specific state with the aim of holding that state legally responsible for the violation of an obligation pursuant to international law.

In the case of legal attribution a distinction must be made between operations carried out by or on behalf of a state and operations carried out by non-state actors. An act by a government body in its official capacity (for example the National Cyber Security Centre) is always attributable to the state. An act by a non-state actor is in principle not attributable to a state. However, the situation changes if a state has effective control over the act or accepts it as its own act after the fact. In such a case, the non-state actor (or 'proxy') carries out the operation on the instructions of, or under the direction or control of that state. The threshold for establishing effective control is high. A financial contribution to the activities of a non-state actor, for example, is not sufficient.

In order to attribute a cyber operation it is not required that a state disclose the underlying evidence. Evidence in the legal sense becomes relevant only if legal proceedings are instituted. A state that takes countermeasures or relies on its inherent right of self-defence (see below) in response to a cyber operation may eventually have to render account for its actions, for example if the matter is brought before the International Court of Justice. In such a situation, it must be possible to provide evidence justifying the countermeasure or the exercise of the right of self-defence. This can include both information obtained through regular channels and intelligence.

Under international law there is no fixed standard concerning the burden of proof a state must meet for (legal) attribution, and thus far the International Court of Justice has accepted different standards of proof. The CAVV and the AIV rightly observe as follows in this regard: 'International law does not have hard rules on the level of proof required but practice and case law require sufficient certainty on the origin of the attack and the identity of the author of the attack before action can be taken.'[163]

In the government's view, the burden of proof will indeed vary in accordance with the situation, depending on the seriousness of the act considered to be in breach of international law and the intended countermeasures.

States' response options

International law provides states with various options for responding to conduct by another state in cyberspace. The options available in a particular case depend on

[163] 'Cyber Warfare', No 77, AIV/ No. 22, CAVV December 2011, p. 22.

the specific circumstances. Below the government sets out the main response options available.

Retorsion

Retorsion relates to acts that, while unfriendly, are not in violation of international law. This option is therefore always available to states that wish to respond to undesirable conduct by another state, because it is a lawful exercise of a state's sovereign powers. States are free to take these kinds of measures as long they remain within the bounds of their obligations under international law.

A state may respond to a cyber operation by another state, for example, by declaring diplomats 'persona non grata', or by taking economic or other measures against individuals or entities involvedin the operation. Another retorsion measure a state may consider is limiting or cutting off the other state's access to servers or other digital infrastructure in its territory, provided the countries in question have not concluded a treaty on mutual access to digital infrastructure in each other's territory.

Countermeasures

If a state is the victim of a violation by another state of an obligation under international law (i.e. an internationally wrongful act), it may under certain circumstances take countermeasures in response.[164] Countermeasures are acts (or omissions) that would normally constitute a violation of an obligation under international law but which are permitted because they are a response to a previous violation by another state. In cyberspace, for example, a cyber operation could be launched to shut down networks or systems that another state is using for a cyberattack. A countermeasure is different to the practice of retorsion in that it would normally be contrary to international law. For this reason, countermeasures are subject to strict conditions, including the requirement that the injured state invoke the other state's responsibility. This involves the injured state establishing a violation of an obligation under international law that applies between the injured state and the responsible state, and requires that the cyber operation can be attributed to the responsible state. In addition, the injured state must in principle notify the other state of its intention to take countermeasures. However, if immediate action is required in order to enforce the rights of the injured state and prevent further damage, such notification may be dispensed with. Furthermore, countermeasures must be temporary and proportionate, they may not violate any fundamental human rights, and they may not amount to the threat or use of force.

Necessity

Necessity is a ground justifying an act which, under certain strict conditions, offers justification for an act that would otherwise be deemed internationally wrongful, such as deploying offensive cyber capabilities against another state. A state may invoke necessity if the following conditions are met:

– there is an immediate and serious threat to an essential interest of the state concerned;

– there is no other way to respond to this threat other than to temporarily suspend compliance with one or more of the state's obligations under international law;

[164] For a more detailed discussion of the concept of countermeasures, see the letter of 13 April 2011 from the Minister of Foreign Affairs to the House of Representatives, Parliamentary Papers, House of Representatives, 2010/11, 32 500 V, no. 166.

– the temporary non-compliance does not constitute a serious interference with the essential interests of another state towards which the obligation under international law exists or of the international community, and invocation of necessity in regard to this specific obligation is permitted under international law;[165]

– the state itself has not contributed to the situation of necessity.

Thus, the ground of necessity may be invoked only in exceptional cases where not only are there potentially very serious consequences, but there is also an essential interest at stake for the state under threat. What constitutes an 'essential interest' is open to interpretation in practice, but in the government's view services such as the electricity grid, water supply and the banking system certainly fall into this category.

As regards the 'very serious consequences' required for establishing the existence of a situation of necessity, it should be noted that the damage does not already have to have taken place, but it must be imminent and objectively verifiable. There is no established standard on the degree to whichthe damage in question can be deemed sufficiently serious to justify invoking the ground of necessity. This must be determined on a case-by-case basis. Damage that merely amounts to an impediment or inconvenience is not sufficient. The damage caused or threatened does not necessarily have to be physical: situations in which virtually the entire internet is rendered inaccessible or where there are severe shocks to the financial markets could be classified as circumstances in which invoking necessity may be justified. Equally, establishing the existence of a situation of necessity does not require a state to determine the precise origin of the damage or whether another state can be held responsible for it. This ground for justification is primarily aimedat giving a state the opportunity to protect its own interests and minimise the damage it suffers.

A state that invokes a situation of necessity has limited options for taking action. This ground may be invoked in respect of violations of obligations under international law only provided there is no other real possibility of taking action to address the damage caused or threatened, and provided there is no interference with the essential interests of another state or of the international communityas a whole.

Self-defence

A state targeted by a cyber operation that can be qualified as an armed attack may invoke its inherent right of self-defence and use force to defend itself.[166] This right is laid down in article 51 of the UN Charter. This therefore amounts to a justification for the use of force that would normally be prohibited under article 2(4) of the UN Charter.[167] For this reason strict conditions are attached to the exercise of the right of self-defence.

An armed attack is not the same as the use of force within the meaning of article 2(4) of the UN Charter (see above). In the *Nicaragua* case, the International Court of Justice defined an armed attack as the most serious form of the use of force. This implies that not every use of force constitutes an armed attack.

[165] In the case of some obligations under international law, invoking a ground justifying an act in violation of the obligation is not permitted. These are known as the peremptory norms of international law, such as the prohibition of genocide.

[166] Article 51 of the Charter of the United Nations, San Francisco, 26 June 1945.

[167] The term 'prohibition of the use of force' is explained on page 57.

To determine whether an operation constitutes an armed attack, the scale and effects of the operation must be considered.[168] International law is ambiguous on the precise scale and effects an operation must have in order to qualify as an armed attack. It is clear, however, that an armed attack does not necessarily have to be carried out by kinetic means. This view is in line with the Nuclear Weapons Advisory Opinion of the International Court of Justice, in which the Court concluded that the means by which an attack is carried out is not the decisive factor in determining whether it constitutes an armed attack. The government therefore endorses the finding of the CAVV and the AIV that 'a cyber attack that has comparable consequences to an armed attack (fatalities, damage and destruction) can justify a response with cyber weapons or conventional weapons (...)'. There is therefore no reason not to qualify a cyberattack against a computer or information system as an armed attack if the consequences are comparable to those of an attack with conventional or non-conventional weapons.

At present there is no international consensus on qualifying a cyberattack as an armed attack if it does not cause fatalities, physical damage or destruction yet nevertheless has very serious non- material consequences.

The government endorses the position of the International Court of Justice, which has observed that an armed attack must have a cross-border character. It should be noted that not all border incidents involving weapons constitute armed attacks within the meaning of article 51 of the UN Charter. This depends on the scale and effects of the incident in question.[169]

The burden of proof for justifiable self-defence against an armed attack is a heavy one. The government shares the conclusion of the CAVV and the AIV that 'No form of self-defence whatever may be exercised without adequate proof of the origin or source of the attack and without convincing proof that a particular state or states or organised group is responsible for conducting or controlling the attack.'[170] States may therefore use force in self-defence only if the origin of the attack and the identity of those responsible are sufficiently certain. This applies to both state and non-state actors.

When exercising their right of self-defence, states must also meet the conditions of necessity and proportionality. In this regard the government shares the view of the CAVV and the AIV that invokingthe right of self-defence is justifiable only *'provided the intention is to end the attack, the measures do not exceed that objective and there are no viable alternatives. The proportionality requirement rules out measures that harbour the risk of escalation and that are not strictly necessary to end the attack or prevent attacks in the near future.'*

[168] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), International Court of Justice (ICJ), 27 June 1986, para. 195.

[169] Ibid.

[170] 'Cyber Warfare', No 77, AIV/ No 22, CAVV December 2011, p. 22.

Norway

[Original: English]

1. Introduction

International law applies in cyberspace. This has been recognised by the international community. The 2012-2013 United Nations Group of Governmental Experts (GGE)[171] concluded as much in its consensus report, and wrote as follows:

> 'International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.'[172]

This was reconfirmed in the subsequent consensus report by the 2015 GGE, which also underscored that the UN Charter applies in its entirety.[173] The UN General Assembly welcomed the 2015 report of the GGE in its resolution 70/237 and called upon Member States to be 'guided in their use of information and communications technologies' by the report.

In the Final Substantive Report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG), all UN Member States reaffirmed the conclusions of previous GGEs that international law applies in cyberspace.[174] Moreover, the report called upon States 'to avoid and refrain from taking any measures not in accordance with international law, and in particular the Charter of the United Nations.' The report also concluded that 'further common understandings need to be developed on how international law applies to State use of ICTs.'

Compliance with international law is fundamental for preserving international peace and security in cyberspace. In this paper, Norway sets out its views on the concrete application of certain rules of international law to State conduct in cyberspace, including practical examples, to contribute to a common understanding among States.

The focus of this paper is on cyber activity that threatens international peace and security, and on issues of State sovereignty. However, numerous bilateral and multilateral treaties are also binding on States, and cyber activity perpetrated by or attributable to a State also has the potential to violate such obligations.

2. The application of international law in cyberspace

Key message: International law applies in cyberspace.

Existing international law, that is customary international law and international treaties, has not been developed with cyberspace in mind. However, the application of the rules of international law to new areas, for example in response to technological developments, is nothing new. If the law in certain areas is perceived as unclear when applied to activities in cyberspace, this must be resolved in the usual way through

[171] UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.

[172] See UN Doc., 24 June 2013, A/68/98*, para. 19.

[173] See UN Doc., 22 July 2015, A/70/174.

[174] See UN Doc., 12 March 2021, A/AC.290/2021/CRP.2 para. 34.

interpretation. This applies both to general international law, for instance the rules that relate to sovereignty and state responsibility, and to the specialised regimes of international law, such as international human rights law and international humanitarian law.

Norway is of the view that there is no need for specific legal instruments to set out rights and obligations of States in respect of activities in cyberspace.

3. Cyber operations in violation of international law

Key message:
One of the conditions for holding a State internationally responsible for a cyber operation is that the operation, or the failure to react against the operation, constitutes a breach of an international obligation of the State.

Cyber operations can vary widely in scope and intensity, from minor digital disruptions to armed attacks on a State. One of the conditions for holding a State internationally responsible for a cyber operation is that the operation, or the failure to react against the operation, constitutes a breach of an international obligation of the State.[175] The obligation in question may follow from customary international law or be treaty-based. A cyber operation is thus not unlawful per se but may become so when carried out to the detriment of the rights of other States.

In the following, Norway gives its interpretation of certain obligations of international law as they apply to cyber operations.[176] The focus in Section 3 is on sovereignty, non-intervention and the prohibition on the use of force. The question of attribution of conduct to a State, which is the other condition for holding a State internationally responsible for a cyber operation, is dealt with in Section 4 (State responsibility). The measures a targeted State is entitled to use in response under international law are dealt with in Section 5 (Response measures). Section 6 discusses international humanitarian law as it applies to cyber operations in armed conflict, and Section 7 deals with the application of international human rights obligations in cyberspace.

3.1. Sovereignty

Key message:

Sovereignty is not just a principle, but also a primary rule of international law.

A State must not conduct cyber operations that violate another State's sovereignty.

Whether a cyber operation violates the target State's sovereignty depends on the nature of the operation, the scale of the intrusion and its consequences, and must be assessed on a case-by-case basis.

[175] This is set out as one of two conditions in Article 2 of the International Law Commission's Articles on State Responsibility (ILC ASR). The Article is considered to express customary international law.

[176] This position paper does not contain any specific analysis of cyber espionage, that is cyber operations whose purpose and effect is limited to the mere collection of information for use by the authorities, which is not in itself illegal under international law. However, certain aspects of such intelligence operations could violate specific rules of international law.

The principle of sovereignty is one of the fundamental principles of international law and applies in cyberspace.[177] It refers to the supreme authority of every State within its territory to the exclusion of other States, and also in its relations with other States.

The internal dimension of a State's sovereignty includes the exclusive right to exercise jurisdiction within its territory, including over the information systems located on its territory, and to exercise independent State powers. The external dimension includes the right of the State to decide its foreign policy and to enter into international agreements. Both dimensions of sovereignty apply in cyberspace, subject only to obligations under international law.

Norway is of the view that sovereignty constitutes both an international law principle from which various rules derive, such as the prohibition of intervention and the prohibition of the use of force, and a primary rule in its own right capable of being violated.[178] Thus, cyber operations that do not amount to a prohibited intervention or a prohibited use of force may nevertheless amount to a violation of a State's sovereignty under international law.

The International Court of Justice (ICJ) has consistently held that States have an obligation to respect the territorial integrity and political independence of other States as a matter of international law. In a cyber context this means that a State must not conduct cyber operations that violate another State's sovereignty.

A cyber operation that manifests itself on another State's territory may, depending on its nature, the scale of the intrusion and its consequences, constitute a violation of sovereignty.

Causing physical damage by cyber means on another State's territory may easily qualify as a violation of territorial sovereignty. For example, a cyber operation against an industrial control system at a petrochemical plant that led to a malfunction and a subsequent fire would constitute a violation of the State's territorial sovereignty. In addition to physical damage, causing cyber infrastructure to lose functionality may also be taken into consideration and may amount to a violation. This includes the use of crypto viruses to encrypt data and thus render them unusable for a substantial period of time.

The principle of sovereignty encompasses cyber infrastructure located in a State's territory irrespective of whether it is governmental or private.

Similarly, a cyber operation that interferes with or usurps the inherently governmental functions of another State may constitute a violation of sovereignty.[179]

This is based on the premise that a State enjoys the exclusive right to exercise within its territory, 'to the exclusion of any other State, the functions of a State'.[180] Accordingly, what matters is not whether physical damage, injury, or loss of functionality has resulted, but whether the cyber operation has interfered with data or

[177] Island of Palmas case (USA v Netherlands), arbitral award, 4 April 1928: 'Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State', p. 838.

[178] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), 'Nicaragua case', International Court of Justice (ICJ), judgment 27 June 1986, paras. 15, 212-213 and 292.

[179] See Tallinn Manual 2.0, commentary to Rule 4, p. 21-22, paras. 15-16.

[180] *Island of Palmas* arbitral award, p. 838.

services that are necessary for the exercise of inherently governmental functions. Cases in point would include altering or deleting data or blocking digital communication between public bodies and citizens so as to interfere with the delivery of social services, the conduct of elections, the collection of taxes, or the performance of key national defence activities. Another example could be the manipulation of police communications so that patrol cars are unable to communicate with police dispatch/operation centres. In this context it is irrelevant whether the inherently governmental function is performed by central, regional or local governments and authorities, or by non-governmental bodies in the exercise of powers delegated by such governments or authorities. Conducting elections is a clear example of an inherently governmental function. In contrast to the case of a cyber operation in breach of the prohibition of intervention, there is no requirement for the interference to reach to the level of coercion.

The precise threshold of what constitute a cyber operation in violation of sovereignty is not settled in international law, and will depend on a case-by-case assessment.

3.2 The prohibition of intervention

Key message:

Cyber operations that compel the target State to take a course of action, whether by act or omission, in a way that it would not otherwise voluntarily have pursued (coercion) in matters relating to its internal or external affairs (*domaine réservé*), will constitute an intervention in violation of international law.

The prohibition of intervention applies to a State's cyber operations as it does to other State activities.[181] Accordingly, a State must not carry out cyber operations in breach of the prohibition of intervention, according to customary international law.[182]

A cyber operation must therefore not be carried out to compel the target State to take a course of action, whether by act or omission, in a way that it would not otherwise voluntarily have pursued (coercion) in matters relating to its internal or external affairs (*domaine réservé*) – such as a State's political, economic, social or cultural system or the formulation of its foreign policy.[183] The constituent element of coercion means that cyber activities that are merely influential or persuasive will not qualify as illegal intervention.

Holding elections is an example of a matter within a State's *domaine réservé*. Thus, carrying out cyber operations with the intent of altering election results in another State, for example by manipulating election systems or unduly influencing public opinion through the dissemination of confidential information obtained through cyber operations ('hack and leak'), would be in violation of the prohibition of intervention. Another example is a cyber operation deliberately causing a temporary shutdown of the target State's critical infrastructure, such as the power

[181] Norway recognises that no State seems to object to the application of the prohibition on intervention (or rule of non-intervention) in the cyber context. Reference is made to the GGE 2015 report, para. 26 and 28(b), subsequently endorsed by the GA. However, Norway is aware that there are differences of opinion as to where the threshold for breach lies.

[182] *Nicaragua* judgment, para. 202.

[183] *Nicaragua* judgment, para. 205.

supply or TV, radio, Internet or other telecommunications infrastructure in order to compel that State to take a course of action.

3.3 Prohibition on the use of force

Key message:

A cyber operation may, depending on its scale and effects, violate the prohibition on the threat or use of force in Article 2(4) of the UN Charter.

A cyber operation that is in violation of the prohibition on the threat or use of force may, depending on its scale and effects, constitute an armed attack under international law. An armed attack is the gravest form of the use of force.

Article 2(4) of the UN Charter prohibits the threat or use of force by a State against the territorial integrity or political independence of another State, or in any other manner inconsistent with the purposes of the UN. The prohibition is a norm of customary international law.[184] It applies to any use of force, regardless of the weapons or means employed.[185]

There are only three exceptions to the prohibition on the use of force in the sense that using force would not be in violation of international law: if the state on whose territory the use of force takes place consents; if it is authorised by the Security Council under Chapter VII of the UN Charter; or in the case of self-defence, in response to an armed attack as recognised in Article 51 of the UN Charter.

Whether a cyber operation violates the prohibition on the threat or use of force in Article 2(4) of the UN Charter depends on its scale and effects, physical or otherwise.[186] Depending on its gravity, a cyber operation may also constitute an armed attack under international law.[187,188] In accordance with the case law of the International Court of Justice (ICJ), an armed attack is the gravest form of the use of force.[189]

A cyber operation may constitute use of force or even an armed attack if its scale and effects are comparable to those of the use of force or an armed attack by conventional means. This must be determined based on a case-by-case assessment having regard to the specific circumstances. A number of factors may be taken into consideration, such as the severity of the consequences (the level of harm inflicted), immediacy, directness, invasiveness, measurability, military character, State involvement, the nature of the target (such as critical infrastructure) and whether this

[184] *Nicaragua* judgment, paras. 188-190.

[185] See *Legality of the Threat or Use of Nuclear Weapons*, ICJ, advisory opinion 8 July 1996, para. 39.

[186] *Nicaragua judgment,* para. 195, where ICJ stated that the 'scale and effects' are to be considered when assessing whether particular actions constitute an 'armed attack'. The factors are equally useful and logical when determining whether a cyber operation constitutes the use of force according to Article 2(4) of the UN Charter.

[187] *Nicaragua* judgment, para. 195.

[188] A cyber operation that constitutes an armed attack on a State under international law triggers the right to self-defence under Article 51 of the UN Charter. See *Section 5 Response measures* in this paper.

[189] *Nicaragua* judgment, para. 191: '[. . .] it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms'.

category of action has generally been characterised as the use of force.[190] This list is not exhaustive.

Cyber operations that cause death or injury to persons or physical damage to or the destruction of objects could clearly amount to the use of force. Likewise, a cyber operation causing severe disruption to the functioning of the State such as the use of crypto viruses or other forms of digital sabotage against governmental or private power grid- or telecommunications infrastructure, or cyber operations leading to the destruction of stockpiles of Covid-19 vaccines, could amount to the use of force in violation of Article 2(4). Similarly, the use of crypto viruses or other forms of digital sabotage against a State's financial and banking system, or other operations that cause widespread economic effects and destabilisation, may amount to the use of force in violation of Article 2(4).

A cyber operation that severely damages or disables a State's critical infrastructure or functions may furthermore be considered as amounting to an armed attack under international law. Depending on its scale and effect, this may include a cyber operation that causes an aircraft crash.

4. State responsibility

Key message:

In order for a State to be held internationally responsible for a cyber operation, the operation has to be attributable to the State under international law.

A State may also be held responsible under international law if it possesses knowledge of a cyber operation that is being carried out from its territory and causing serious adverse consequences with respect to a right of the target State under international law, and fails to take reasonably available measures to terminate the cyber operation.

The general rules on State responsibility under international law apply to cyber operations just as they apply to other activities.

In order for a State to be held responsible for a cyber operation under international law, it is a condition that the cyber operation is attributable to the State under international law.[191] Both State and non-State actors conduct cyber operations. Even if a cyber operation is not conducted by someone acting directly or indirectly on behalf of a State, the State may nevertheless be held responsible under international law if it fails to take adequate measures against cyber operations that target third States from or via its territory.

4.1. Attribution under international law

A State may be held responsible under international law for cyber operations conducted by an organ of the State or by actors exercising governmental authority on behalf of the State.[192]

[190] Tallinn Manual 2.0., commentary to Rule 69, p. 333-337, paras. 9-10.

[191] The condition is set out in Article 2 ILC ASR. The other condition, that the act or omission must constitute a breach of an international obligation of the State, is dealt with in Section 3.

[192] Cf. ILC ASR, in particular Articles 4, 5 and 7.

A State may be held responsible under international law for cyber operations conducted by non-State actors if these are conducted on the direct instructions of the State or under its direction or effective control.[193] It may be technically challenging to establish that a relationship between a State and a non-State actor amounts to direct instructions, direction or effective control. However, this is a question of evidence, and not of lack of clarity of international law.

4.2. Due diligence

Furthermore, a State may be held responsible under international law if it knows or should have known that cyber operations that target third States are being carried out from or via its territory, and fails to take adequate measures.[194]

As a consequence of the right to exercise sovereignty over cyber infrastructure located on its territory, States also have a corresponding obligation not to knowingly allow their territory to be used for acts causing significant harm to the rights of other States under international law. This customary international law obligation, often referred to as the due diligence principle, was recognised by the ICJ in the 1949 Corfu Channel judgment,[195] and is reflected in numerous rules in specialised regimes of international law. Norway is of the view that the due diligence obligation applies in situations where there is a risk of transboundary harm from hazardous activities, regardless of the nature of the activity, and accordingly also applies to cyber operations.

Accordingly, if a State possesses knowledge of a cyber operation being carried out from or via its territory causing serious adverse consequences with respect to a right of the target State under international law, it is required to take adequate measures to address the situation.

The due diligence standard is the conduct that is generally considered to be appropriate and proportional to the degree of risk of transboundary harm in the particular instance. It is an obligation of conduct, not of result. Applied to cyber activities, what is required is for the State to take all reasonably available measures to terminate the cyber operation. A breach of the obligation consists not of failing to achieve the desired result, but of failing to take the necessary, diligent steps towards that end. It is irrelevant whether the cyber operation in question is conducted by a third State or a non-State actor. Likewise, it is irrelevant whether the cyber operation in question is conducted by an actor physically present on the State's territory or by an actor making remote use of ICT infrastructure on the State's territory.

In addition to actual knowledge of the use of cyber infrastructure within its territory for harmful cyber operations against another State, a State may also violate its due diligence obligation if it is in fact unaware of the activities in question but objectively should have known about them and fails to address the situation.[196] Accordingly, knowledge also encompasses those situations in which a State in the normal course of events would have become aware that its territory was being used

[193] See Article 8 ILC ASR. See also *Nicaragua* judgment, para 115, and *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, ICJ, judgment 27 February 2007, para. 400.

[194] See Article 2 ILC ASR, which explicitly states that a State's conduct may consist of 'an action or omission'. See also *Corfu Channel,* ICJ, judgment 9 April 1949, p. 18.

[195] *Corfu Channel* judgment, 9 April 1949, p. 22.

[196] *Corfu Channel* judgment, 9 April 1949, p. 18.

for harmful cyber operations.[197] This implies that the criterion that a State 'should have known' is more likely to be met if for instance the operation used publicly known and easily detected malware, as opposed to highly sophisticated and previously unknown malware.

There is currently no legal basis for a general obligation to prevent cyber operations, and States are consequently not under an obligation to monitor all cyber activities on their territories.[198]

Norway considers the due diligence obligation to be of particular importance in a cyber context. In situations where a targeted State cannot directly attribute (technically and legally) a wrongful cyber operation – for instance election interference – to the State from whose territory it is being carried out, the territorial State may nevertheless still be held accountable on the basis of a breach of the due diligence obligation.

5. Response measures

The response measures an injured State may take under international law depend on the severity and nature of the cyber operation and on whether the legally responsible actor behind it is another State or a non-State actor.

5.1 Retorsion

A State may respond to any form of cyber operation by retorsion. Retorsion refers to the taking of measures that are lawful but unfriendly, directed against another State. Retorsion may therefore be used regardless of whether international law has been violated and regardless of whether State responsibility applies. Examples of acts of retorsion are breaking off or limiting diplomatic relations, for instance by declaring a diplomat persona non grata, or the imposition of sanctions. Publicly declaring that another State is responsible for a cyber operation is in itself an act of retorsion.

5.2 Countermeasures

If a State is the victim of an internationally wrongful cyber operation and another State can be held responsible under customary international law on State responsibility, the injured State may, depending on the circumstances, be entitled to take countermeasures.

A countermeasure is an act that would otherwise be contrary to international law, but where the injured State can invoke the prior internationally wrongful act[199] as a ground for precluding wrongfulness.[200] If there is doubt regarding the attribution of a cyber operation to a State under international law, it may be preferable for the injured State to make use of acts of retorsion rather than countermeasures in order to avoid the possibility of incurring State responsibility for its response.

Countermeasures may only be taken to induce a State to cease an internationally wrongful act or resume its compliance with an international obligation. They are not to be used for punishment and retaliation. Countermeasures must be limited to what is considered necessary and proportional, and may only target the State to which the

[197] See also Tallinn Manual 2.0, commentary to Rule 6, p. 41.

[198] A general obligation of full control and prevention in the cyber context could be problematic in relation to a State's obligations under international human rights law.

[199] In this document, 'internationally wrongful acts' must be understood as including both actions and omissions, see Articles 1 and 2 ILC ASR.

[200] See Articles 22 and 49–54 ILC ASR.

cyber operation or internationally wrongful act can be attributed. There is no requirement for countermeasures to be of the same nature as the internationally wrongful acts to which they are a response, and countermeasures in response to cyber operations may therefore be carried out within or outside cyberspace. Countermeasures must not violate the prohibition on the threat or use of force or international humanitarian law.

The State held responsible should be notified of both the violation of international law and the grounds for attribution, as well as of the intention to introduce countermeasures.[201] Countermeasures may only be taken if a State has sufficient grounds for attributing the conduct in question to a particular State under international law. What constitutes sufficient grounds will be fact-specific and case-specific, and can be particularly challenging to determine in the case of cyber operations. The State taking countermeasures must be confident in its attribution before resorting to countermeasures. However, the State taking countermeasures need not publish detailed grounds for its attribution or give a detailed technical account of this to the State identified as responsible as this might reveal sensitive methods of interception and detection or offensive and defensive capabilities.

Countermeasures may be taken without prior notification to the responsible State if providing such notification might reveal sensitive methods or capabilities or prevent the countermeasures from having the necessary effect. For example, the injured State could carry out a cyber operation to disrupt the capability of the aggressor State conducting the internationally wrongful cyber operation such as election interference. This countermeasure would in other circumstances be in violation of the aggressor State's sovereignty.

5.3 Necessity

In a situation of necessity, a State may be able to respond to a cyber operation in a way that is in principle in breach of an international obligation and nevertheless not incur responsibility for its actions under international law.

Necessity refers to those exceptional situations where the only way a State can safeguard an essential interest threatened by a grave and imminent peril, whether cyber in nature or not, is by temporary non-compliance with international obligations of lesser weight or urgency. For instance, if infrastructure in a third country is used in an internationally wrongful cyber operation, the injured State may under certain conditions launch a cyber operation to destroy or disrupt the internationally wrongful cyber operation, even if this violates the territorial sovereignty of the third State.

It is not a requirement that the preceding cyber operation must be attributable to a particular State.

It should be emphasised that, according to customary law on state responsibility, a number of conditions must be fulfilled before necessity can be invoked as a ground for precluding wrongfulness.[202]

5.4 Self-defence

A State that is the victim of a cyber operation that qualifies as an armed attack under international law, may exercise its inherent right of individual or collective self-defence under Article 51 of the UN Charter.

---

[201] ILC ASR Articles 43 and 52.

[202] See Article 25 ILC ASR.

The right of self-defence as reflected in Article 51 is a norm of customary international law. It must be exercised subject to the requirements of necessity and proportionality[203], and may involve both digital and conventional means.

6. Cyber operations during armed conflicts – international humanitarian law

Key message:

International humanitarian law applies to cyber operations in connection with an armed conflict.

International humanitarian law (IHL) applies in the event of an armed conflict. Whether an (international or non-international) armed conflict exists will depend on the specific circumstances.

This specialised regime of international law, also called *jus in bello*, governs actions, including cyber operations, when they are conducted in connection with an armed conflict.

International humanitarian law aims to minimise the human suffering caused by armed conflict. It thus regulates and limits cyber operations during armed conflicts, just as it regulates and limits the use of any other weapons, means and methods of warfare in an armed conflict.

IHL does not legitimise the use of force in cyberspace. Any use of force by States – either by digital or by conventional means – remains governed by the Charter of the United Nations and the relevant rules of customary international law, also called *jus ad bellum*. Of particular relevance is the prohibition against the use of force. International disputes must be settled by peaceful means, in cyberspace as in all other domains.

The general rules for legitimate military targets are the same regardless of whether conventional or digital means are used. A cyber operation conducted in connection with an armed conflict must be assessed according to its consequences, and may qualify as an attack under international humanitarian law. 'Attack' is a key concept of international humanitarian law, and is understood to mean 'acts of violence against the adversary, whether in offence or defence'.[204] Cyber attacks during armed conflicts are subject to the same restrictions and regulations under international humanitarian law as conventional attacks, including the principles of humanity, military necessity, proportionality and distinction. The concept of attack is particularly relevant to the rules and principles on the selection of targets and precautions. Attacks against civilians or civilian objects are for example prohibited.[205]

Under IHL, medical services must be protected and respected, including when carrying out cyber operations during armed conflict.[206] IHL also prohibits attacking,

[203] See e.g. *Nicaragua* judgment paras. 176, 194, and *Oil Platforms,* ICJ, judgement 6 November 2003, paras. 43, 73-74, 76.

[204] Additional Protocol I to the Geneva Conventions of 12 August 1949 relating to the protection of victims of international armed conflict (AP I), Article 49(1).

[205] AP I, Article 51(2) and 52(1).

[206] See, for instance, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (GCI), Article 19; Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (GCII), Article 12; Convention

destroying, removing or rendering useless objects indispensable to the survival of the population, including through cyber means and methods of warfare.[207] 'Objects indispensable to the survival of the civilian population' include ICT infrastructure for food production or drinking water installations.

7. Human rights in cyberspace

Key message:

States must comply with their human rights obligations in cyberspace, just as they must in the physical world. States must both respect and protect human rights.

International human rights law applies to cyber activities just as it does to any other activity. States must comply with their human rights obligations also in cyberspace, as they must in the physical world. States must both respect and protect human rights, including the right to freedom of expression and the right to privacy.

Neither the individuals that are subject to a State's jurisdiction, nor the concept of jurisdiction, is altered by the fact that the activity attributed to the State is a cyber activity. In this respect, cyber activity is no different from other means that States may use to violate their human rights obligations towards their citizens.

(IV) relative to the Protection of Civilian Persons in Time of War (GCIV), Article 18; AP I, Article 12; AP II, Article 11; ICRC Customary IHL Study, Rules 25, 28, 29.

[207] AP I, Article 54; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (AP II), Article 14; ICRC Customary IHL Study, Rule 54.

Romania

[Original: English]

General remarks

The full respect for the international law is one of the most important pillars of Romania's foreign policy. It is our belief that international relations, irrespective of the tools used, must be based on international law. This is true as well for cyberspace.

An open, secure, stable, accessible and peaceful online environment and a responsible State behaviour in cyberspace cannot be imagined outside an international rules-based system, primarily founded on international law.

Given the specificities of cyberspace and of the incident of various information and communication technologies, the discussion on how international law applies in cyberspace is a complex one.

However, the fact that there is a need to further discuss on how exactly international law applies to cyberspace does not mean that international law does not apply to cyberspace and that we are facing a legal vacuum.

State practice will in time further crystalize the application of international law in cyberspace; as a matter of fact, not all aspects can or even should be clarified in detail in absence of relevant state practice. This is however, without prejudice to the obligation of States to act in a responsible manner including in cyberspace and assume conduct that is in line with general international law.

Romania is of the strong opinion that existing **international law equally applies to cyberspace** and that there is no need to develop international legal frameworks to address strictly cyberspace.

This paper tackles upon some major aspects of international law in relation to cyberspace. They concern inter-State relations in cyber contexts, given that international law applies to States and governs the relations between them.

State sovereignty

One of the issues on which discussions need to focus more is the respect for state sovereignty in the context of cyber operations.

Romania considers that respect for the state sovereignty is an international obligation *per se*, the breach of which constitutes an internationally wrongful act; States have an obligation to respect the sovereignty of other States and refrain from activities that constitute a violation of their sovereignty; this holds true both in what concerns the internal as well as the external facet of the principle of sovereignty.

At the same time, we acknowledge that the difficulty in relation to this principle lies in the absence in cyberspace context of the territoriality and physical dimensions[208], which are the specific elements of the analysis when dealing with the sovereignty in the traditional sense.

In relation to these aspects, RO is of the view that cyber operations (*conducted by a State organ or by a person or entity exercising elements of governmental authority or by a person acting under the instructions of or under the direction or control of a State*) that interferes with or prevents in any way a State from exercising its (internal and/ or external) sovereign prerogatives (i.e. authority over its territory,

[208] The principle refers to protecting the state authority over property and persons within its own ***national borders***.

over the property and persons situated therein) constitute a violation of the principle of State sovereignty and, thus, a breach of international law.

If there is not a State or State endorsed operation one can speak of a criminal act, which should be investigated and punished in accordance with the criminal law of the State concerned.

Due diligence principle

The due diligence principle entails that a State may be responsible for the effects of the conduct of private persons, if it failed to take necessary measures to prevent those effects[209].

This principle (which implies a certain obligation of conduct on the part of States) was enunciated by the ICJ in its Corfu Channel judgment[210] emphasizing that every State is under an "obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".

The due diligence principle requires that States take action in respect of cyber activities if the following elements are cumulatively met:

- ✓ the acts are conducted by a non-State actor or a third State) from or through the territory of the potentially responsible State (or from or through the territory or cyber infrastructure under its control);
- ✓ the acts are contrary to the rights of a victim State and have serious adverse consequences for that State;
- ✓ the State has actual or constructive knowledge of those acts.

Non-Intervention

In connection with this principle, the principle of prohibition of the intervention in the internal affairs of another State should be addressed (situations of tampering with the electoral processes in other States are relevant as a discussion under this principle).

According to international law, States are under the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter; this means that no State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State.

In order for such intervention to be illegal under international law, it must be coerced, meaning that the goal of the intervention must be to effectively change the behavior of the target State; the incidence of coercion must be assessed on a case-by-case basis, in order to determine the violation of the principle of non-intervention.

In other words, the following criteria must be met in order for an act to qualify as prohibited intervention under international law:

- ✓ the act must bear on those matters in which States may decide freely (internal and external affairs – the domain reservé of States);
- ✓ the act must be coercive in nature;
- ✓ there has to be a causal nexus between the coercive act and the effect on the internal or external affairs of the target State.

[209] ILC's Articles on State Responsibility, Chapter II, para. 4.

[210] Corfu Channel Case (UK v Albania) (Merits) [1949] ICJ Rep 4, 22.

Therefore, depending on the situation, interference in the internal or external affairs of Romania (that is interference which causes or may cause harm to Romania's economic, political, social and/ or cultural system) *may* constitute a violation of the principle of non-intervention.

Prohibition of the threat or use of force

The prohibition of the threat or use of force is a well-established principle of international law, being included in art. 2(4) of the UN Charter. There are only three (well determined) exceptions to this prohibition: self-defense in the event of armed aggression, UNSC Chapter VII authorization of the use of force and consent of the State on whose territory the operation takes place.

In order to ascertain whether a cyber operation represents a threat or use of force and whether it even amounts to a cyberattack, a case-by-case analysis must be carried out to determine the circumstance in which the attack occurred, the nature of the operation (military or not) and the scale and the effects of the operation (by comparison against the scale and severity of a conventional (non-cyber) act of violence covered by the prohibition).

The elements of such an analysis, from the "scale and effects" perspective, are well established in the ICJ's relevant jurisprudence.

It is also worth noting that not all cyber operations reach the threshold of use of force and even less operations reach the threshold of an armed attack; nevertheless such operations could still be in violation of international law (being a prohibited intervention or an otherwise violation of the principle of sovereignty).

International humanitarian law

International Humanitarian Law (IHL) applies in the context of cyber operations carried out as part of an armed conflict (whether international or non-international).

In such circumstances, the planning of and carrying on of cyber operations must be done in conformity with the principles governing the conduct of hostilities, namely distinction, proportionality, necessity and precaution.

There are ongoing discussions in relation to qualifying *data* as an object for the purposes of the application of IHL. We take the preliminary view that cyber operations against data do trigger the application of IHL. Therefore cyber-attacks can only be directed against those data that represent military objectives according to IHL and cannot be directed against those data that represent a civilian object which must be protected under the principle of distinction.

We are also of the view that the principle of neutrality apply as well to cyber operations as part of an armed conflict and thus, belligerents must refrain from harming information and communication infrastructure situated on the territory of a neutral State or from launching attacks from such infrastructure.

Human rights law

Human rights are protected similarly both in offline as well in online contexts.

International law does not recognise a right to States to derogate from their international human rights obligations as a defensive-type measure – for instance to restrict access to internet in all circumstance as a responsive measure to counter some types of conduct in cyberspace (which generally pertain to criminal law, like: countering terrorism, violent extremism or fraud).

The circumstances in which limitations to human rights are permitted are well established in international law and apply the same way in offline and in online contexts. In most cases, the factors to be weighted include whether the restriction serves a legitimate purpose, whether it has a legal basis and whether it is necessary and proportionate to the interest it aims to protect.

Therefore, whatever regulation a State adopts (by virtue of its sovereign right) it must conform with its international obligations in the field of human rights. Otherwise it entails its legal responsibility under the relevant international conventions.

It is our view that the existing human rights instruments provide sufficient scope for effectively safeguarding the protection of human rights in cyberspace.

State responsibility[211]

There is an internationally wrongful act of a State when conduct consisting of an action or omission is:

- ✓ attributable to the State under international law; and
- ✓ constitutes a breach of an international obligation of the State.

Therefore, from the perspective of state responsibility under international law, attribution is one of the components.

In cyber context, attribution (especially from the technical point of view) of the conduct to a State is difficult to determine given the fact that most of the times the actions are undertaken via proxies.

Therefore, if the conduct is not evident as being of a State organ, then, in order to be attributed to a State, it must be proven that it is:

- ✓ of a person or entity exercising elements of the governmental authority of that State;
- ✓ of organs placed at the disposal of that State by another State;
- ✓ of a person or entities acting under the instructions of, or under the direction or control of that State.

In order to determine the degree of control reference should be made to the jurisprudence of the ICJ and of the various international courts and tribunals that have dealt with matters of State attribution.

Once attributed to a State and determined that the conduct constitutes a breach of an international obligation (the 2nd component), the international responsibility of that State is entailed and can be invoked by the injured State either individually (if the obligation breached is owed to that State or if that State was otherwise affected by the conduct) or collectively with other States if the obligation breached was owed to a group of States (including that State) or to the international community as a whole; the invocation of the responsibility of a State is a matter of political choice; however, the responsibility of a State for an international wrongful act is an objective circumstance from the legal standpoint, which exists independent of its invocation by the injured State(s); nevertheless, under draft articles of State responsibility there is a certain procedure to be followed by the injured State invoking the responsibility of another State (therefore a pubic invocation may not suffice).

[211] For reference see ILC's Articles on State responsibility which in RO's view largely reflect customary international law.

At the same time, once the international responsibility of a State is entailed, the injured State(s) may recourse to countermeasures in order to induce that State to comply with its international obligations.

Instead of conclusion

It is our firm conviction that there is no reason to consider that the existing international law could not appropriately govern the inter-States relations carried out in cyberspace/ or through the medium of cyberspace.

More dialogue and exchanges among States can help clarifying some of the specific circumstances of the applicability of the international law to cyberspace.

Russian Federation

[Original: English and Russian]

Russia assumes that, for the present, the international community has reached consensus on the applicability of the universally accepted principles and norms of international law, which are enshrined, first and foremost, in the Charter of the United Nations and the Declaration on principles of international law, friendly relations and cooperation among States in accordance with the Charter of the United Nations of October 24, 1970, to information space. These include, in particular, the principles of sovereign equality of States, non-use of force and threat of force, settlement of international disputes by peaceful means, non-interference into internal affairs of States, obligation of States to cooperate with each other, equal rights and self-determination of peoples, fulfillment of international law obligations in good faith, inviolability of State borders, and territorial integrity of States. This understanding was agreed upon at relevant UN platforms on international information security and set forth, inter alia, in the 2013 and 2015 reports of the UN Group of Governmental Experts (GGE) and in the 2021 report of the UN Open-ended Working Group (OEWG), as well as in the UN General Assembly resolution (A/RES/73/27, para. 17 of the preamble) proposed by Russia and adopted in 2018. It is presumed that international obligations of States, including those stemming from international treaties as the main sources of international law, are applicable in information space.

At the same time, given the specific legal nature of the information environment, notably, the fact that activities therein can be anonymous, the application of international law to the use of information and communications technologies (ICTs) should not be automatic and should not be carried out by simple extrapolation. There is a need to substantively discuss the issue of how specific instruments of the existing international law apply to the ICT-sphere, as well as to elaborate a universal approach to this matter under the UN auspices.

The possibility of attributing responsibility for particular actions in information space to States demands further study on the basis of the existing international law. The international responsibility of a State is conditioned to the commission of an internationally wrongful act by this State. According to the Articles on Responsibility of States for Internationally Wrongful Acts (elaborated by the UN International Law Commission in 2001, taken note in the UNGA resolution A/RES/56/83), there is an internationally wrongful act of a State when conduct consisting of an action or omission: 1) is attributable to the State under international law; 2) constitutes a breach of an international legal obligation of the State. The characterization of an act of a State as internationally wrongful is governed by international law. Such characterization is not affected by the characterization of the same act as lawful by internal law (article 3).

The countermeasures, which can be taken by an injured State against a State which is responsible for an internationally wrongful act, shall not affect the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations; obligations for the protection of fundamental human rights; obligations of a humanitarian character prohibiting reprisals; other obligations under peremptory norms of general international law (article 50).

Under customary international law, a State is responsible for activities of its institutions, as well as that of individuals acting under its control. In information space it may be difficult to determine whether an individual is acting under control of a State or with its acquiescence. In this regard, it becomes increasingly relevant to formalize the norm of the 2015 GGE report stating that all accusations of organizing and implementing wrongful acts brought against States should be substantiated, as

legally binding. In any case, one should refrain from publicly imposing responsibility for an incident in information space on a particular State without supplying necessary technical evidence.

Promoting the use of ICTs for peaceful purposes and conflict prevention in this sphere correspond to the interests of all States. These basic principles of State activities in information space are enshrined in the abovementioned 2013 and 2015 GGE reports and 2021 OEWG report, as well as in the General Assembly resolutions adopted by the majority of the UN Member States (namely, A/RES/73/27, A/RES/73/266, A/RES/74/29, A/RES/75/32, A/RES/75/240 and others).

Readiness and political will of States to undertake relevant legal obligations and comply with them are required to ensure effective international legal regulation of the ICT-sphere. In this regard, Russia advocates a broader idea of progressive development and improvement of international law taking into account the specific features of ICTs. Given the cross-border nature of interstate legal relationship in this domain, its legal regulation should be carried out by means of developing and adopting a binding universal convention on international information security at the UN level.

We consider that the international community should continue to undertake an in-depth study of all controversial issues concerning international legal regulation of the ICT-sphere, as well as to elaborate new norms, on a universal and genuinely democratic basis – within the framework of the Russia-initiated Open-ended-Working Group on security of and in the use of ICTs 2021–2025 (pursuant to the UNGA resolution 75/240 of December 31, 2020). The establishment of a thematic subgroup (with participation of international legal experts and academia) will contribute to organizing a domain-specific discussion on this matter.

***

Россия исходит из того, что на данный момент в мировом сообществе сформировался консенсус относительно применимости к информационному пространству общепризнанных принципов и норм международного права, прежде всего, закрепленных в Уставе ООН и Декларации о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом ООН от 24 октября 1970 г. Речь идет, в частности, о принципах суверенного равенства государств, неприменения силы и угрозы силой, разрешения международных споров мирными средствами, невмешательства во внутренние дела государств, обязанности государств сотрудничать друг с другом, равноправия и самоопределения народов, добросовестного выполнения обязательств по международному праву, нерушимости государственных границ, территориальной целостности государств. Данное понимание зафиксировано на профильных ооновских площадках по международной информационной безопасности (МИБ), в частности, в докладах групп правительственных экспертов (ГПЭ) ООН 2013 и 2015 гг. и Рабочей группы ООН открытого состава (РГОС) 2021 гг., а также в принятой по инициативе России в 2018 г. резолюции Генеральной Ассамблеи ООН (A/RES/73/27, п.17 преамбулы). В информационном пространстве презюмируется применение международных обязательств государств, в том числе вытекающих из международных договоров как основных источников международного права.

В то же время, учитывая особую правовую природу информационной среды, в частности, то, что деятельность субъектов в ней может иметь анонимный характер, применение международного права в сфере использования информационно-коммуникационных технологий (ИКТ) не должно происходить автоматически и

путем простой экстраполяции понятий. Востребовано предметное обсуждение вопроса о том, как конкретные инструменты действующего международного права применяются в сфере использования ИКТ, и выработка под эгидой ООН универсального подхода к его решению.

Возможность установления ответственности государств за конкретные действия в информационном пространстве требует дальнейшего изучения с опорой на действующее международное право. Необходимым условием для наступления международной ответственности государства является совершение им международно-противоправного деяния. В соответствии со Статьями об ответственности государств за международно-противоправные деяния (разработаны Комиссией международного права ООН в 2001 г., приняты к сведению резолюцией ГА ООН A/RES/56/83) международно-противоправное деяние государства имеет место, когда какое-либо его поведение, состоящее в действии или бездействии: 1) присваивается государству по международному праву; 2) представляет собой нарушение международно-правового обязательства данного государства. Квалификация деяния государства как международно-противоправного определяется международным правом. На нее не влияет квалификация этого деяния как правомерного по внутреннему праву (ст.3).

Контрмеры, которые потерпевшее государство может принимать против государства, ответственного за международно-противоправное деяние, не могут затрагивать обязательства воздерживаться от угрозы силой или ее применения, закрепленного в Уставе ООН, обязательств по защите основных прав человека, обязательств гуманитарного характера, запрещающих репрессалии, иных обязательств, вытекающих из императивных норм общего международного права (ст.50).

Согласно обычному международному праву государство несет ответственность за деятельность своих органов, а также лиц, которые действуют под контролем государства. Установить, действует ли определенное лицо в информационном пространстве под контролем государства или при его попустительстве, может быть затруднительно. В связи с этим представляется весьма актуальным придание юридически обязательного характера закрепленной в докладе ГПЭ 2015 г. норме, согласно которой все обвинения в организации и совершении противоправных деяний, выдвигаемые против государств, должны быть обоснованными. В любом случае следует воздерживаться от публичного возложения ответственности за какой-либо инцидент в информационном пространстве на конкретное государство без предоставления необходимых технических доказательств.

Интересам всех государств отвечает содействие использованию ИКТ в мирных целях и предупреждению конфликтов, связанных с их применением. Эти базовые принципы деятельности государств в информпространстве закреплены в упомянутых докладах ГПЭ 2013 и 2015 гг. и РГОС 2021 г., а также в принятых большинством государств-членов ООН резолюциях Генеральной Ассамблеи (в частности, A/RES/73/27, A/RES/73/266, A/RES/74/29, A/RES/75/32, A/RES/75/240 и др.).

Для эффективного международно-правового регулирования сферы использования ИКТ необходима готовность и политическая воля государств принимать на себя профильные юридические обязательства и выполнять их. В этой связи Россия выступает за более широкую идею прогрессивного развития и совершенствования международного права с учетом специфики ИКТ. Принимая во внимание трансграничный характер правоотношений государств в этой сфере, ее правовое регулирование должно быть реализовано путем разработки и

последующего принятия на площадке ООН универсальной конвенции в области обеспечения МИБ, которая носила бы обязательный характер.

Исходим из того, что углубленное изучение всего комплекса спорных вопросов международно-правового регулирования сферы использования ИКТ, а также разработка новых норм должна быть продолжена международным сообществом на универсальной и подлинно демократичной основе – в рамках создаваемой по российской инициативе Рабочей группы ООН открытого состава (РГОС) по вопросам безопасности в сфере использования ИКТ и самих ИКТ (в соответствии с резолюцией ГА ООН №75/240 от 31 декабря 2020 г.). Организации специализированной дискуссии по данной теме будет способствовать создание в новой РГОС профильной тематической подгруппы (с участием юристов-международников и научно-академического сообщества).

Singapore

[Original: English]

1. As a small State, Singapore has always supported the rules-based multilateral system and the role of the United Nations ("UN"). The UN provides the foundation for international law, rules, and norms. Multilateral institutions, systems, and laws are critical for the survival of all States, in particular small States.

2. Singapore's approach is no different with regard to cyberspace; we believe it is important to build a rules-based international order in cyberspace, especially given rapid digitalisation. The adherence by States to international law is essential to support and promote an open, secure, stable, accessible, peaceful, and interoperable ICT environment.

3. Singapore affirms the principle that international law, in particular the Charter of the United Nations (the "UN Charter"), applies to cyberspace.

4. This document sets out Singapore's position on the key principles of international law that govern the behaviour of States *inter se* in cyberspace.

Key Principles

5. Singapore affirms that the following key principles enshrined in the UN Charter apply in cyberspace as they do in the physical world, and are of fundamental importance to small States, such as Singapore:

- First, the principles of State sovereignty and sovereign equality of all States. Singapore's position is that a cyber operation could, in certain circumstances, amount to a violation of sovereignty.
- Second, and as a corollary of the first, the principle of non-intervention in each other's internal affairs. Singapore affirms that the principle of non-intervention in the internal affairs of other States applies to cyberspace.

A prohibited intervention by one State against another must have a bearing on matters in which the victim State is permitted, by the principle of State sovereignty, to decide freely, including its choice of a political, economic, social and cultural system, and the formulation of foreign policy. In Singapore's view, intervention necessarily involves an element of coercion. As non-exhaustive examples, where there is interference in Singapore's electoral processes through cyber means, or cyber-attacks against our infrastructure in an attempt to coerce our government to take or forbear a certain course of action on a matter ordinarily within its sovereign prerogative, these instances will constitute a violation of the principle of non-intervention.

- Third, the obligation of all States to settle their international disputes by peaceful means, in such a manner that international peace and security are not endangered.
- Finally, the obligation of all States to refrain from the threat or use of force against the territorial integrity or political independence of any State. A cyber operation can cause severe consequences and effects. In determining whether a cyber operation amounts to the use of force, factors that may be taken into account include, but are not limited to, the prevailing circumstances at the time of the cyber operation, the origin of the cyber operation, the effects caused or sought by the cyber operation, the degree of intrusion of the cyber operation, and the nature of the target.

Right of Self-Defence

6. While Singapore considers the above principles to be essential ones underpinning the international legal order, Singapore's position is that it bears noting that ultimately, none of these impair a State's inherent right of self-defence, as provided under the UN Charter. This right of self-defence also applies in the cyber domain. In other words, a State has the inherent right of self-defence if malicious cyber activity amounting to an armed attack, or an imminent threat thereof, occurs against that State.

7. Malicious cyber activity attributable to a State that causes death, injury, physical damage or destruction equivalent to a traditional non-cyber armed attack, or presenting an imminent threat thereof, would constitute an armed attack. Singapore notes the increasing prevalence of this view amongst States.

8. In Singapore's view, it is also possible that, in certain limited circumstances, malicious cyber activity may amount to an armed attack even if it does not necessarily cause death, injury, physical damage or destruction, taking into account the scale and effects of the cyber activity. An example might be a targeted cyber operation causing sustained and long-term outage of Singapore's critical infrastructure.

9. A series or combination of cyber-attacks, whether or not it is in combination with kinetic attacks, may amount to an armed attack, even if the individual attacks do not reach the threshold equivalent to an armed attack, as long as the attacks are launched by the same actor or by different attackers acting in concert.

Internationally Wrongful Act

10. Even if malicious cyber activity against a State has not risen to the level of an armed attack entitling the victim State to exercise the right of self-defence, international law provides that a victim State that is subjected to another State's internationally wrongful act against it (whether through malicious cyber activity, or physical means) is entitled to have recourse to counter-measures which are consistent with international law.

11. Malicious cyber activity attributable to a State that interferes with a victim State's proper governing functions is an example of an internationally wrongful act.

12. Apart from counter-measures, a victim State that is subject to malicious cyber activity short of an internationally wrongful act may also respond with acts of retorsion.

13. Singapore's view is that the obligation of all States to settle their international disputes by peaceful means, in such a manner that international peace and security are not endangered, remains a key principle underpinning the international legal order.

Due Diligence

14. There is a need for more clarity on the scope and practical applications, if any, of due diligence in cyberspace. Issues such as the threshold required to trigger an obligation on States to act or respond, the degree of knowledge required of States, and the measures expected of a State from which the malicious cyber activity originates, are some examples of the questions that need to be further discussed and addressed among States.

International Humanitarian Law

15. Singapore's view is that in times of armed conflict, the relevant principles of international humanitarian law ("IHL") would apply to the belligerents' use of cyberspace. Some examples of such principles would include those of humanity, necessity, proportionality and distinction.

16. The principle of proportionality requires a State to refrain from launching a cyber operation which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

17. In keeping with the principle of distinction, cyber operations undertaken in the context of armed conflicts have to distinguish between legitimate military objectives and civilian objects. Only legitimate military objectives may be targeted.

Human Rights

18. The same human rights which apply offline also apply online.

Resolution of Disputes

19. Singapore shares the concerns of other States on the escalation of conflicts in the cyber sphere, against the backdrop of continuing fast-paced developments in technology. Singapore affirms the key principle enshrined in the UN Charter that States shall settle their international disputes by peaceful means, in such a manner that international peace and security are not endangered. This obligation applies in cyberspace as it does in the physical world and does not impair the inherent right of States to take measures consistent with international law and as recognised under the UN Charter.

20. Singapore also acknowledges that the novel circumstances brought about by such technological developments will inevitably surface new challenges for the application of international law to activities in cyberspace. To tackle these challenges, Singapore believes in the value of continued discussions within the framework of UN processes to foster common understanding of key rules and principles governing how States should behave in cyberspace.

21. This will deepen trust between members of the international community and provide predictability and stability to States, rather than increase the proliferation of cyber conflicts. Such predictability and stability are essential factors to encourage technological innovation and adoption, investor confidence, and economic progress.

Switzerland

[Original: English and French]

Introduction

In the context of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2019/2021 (UN GGE), the primary focus of states lies on the security-related aspects in the digital space (cybersecurity) and the applicable provisions under international law in this area.[212] The use of the term 'cyberspace' in the present position paper therefore refers only to that part of the digital space which concerns the security dimension. Part I addresses questions concerning international law in general including human rights. Part II places particular emphasis on questions relating to international humanitarian law (IHL).

Switzerland is committed to building and maintaining a free, open, secure and peaceful cyberspace, and to advancing the recognition, observance and enforcement of international law in this space.[213] All states have a common interest in ensuring that cyberspace is governed by the rule of law and used for peaceful purposes only. Switzerland considers international law to be applicable to cyberspace. It therefore welcomes the consensus of previous UN GGEs that international law, and in particular the UN Charter in its entirety, are applicable to cyberspace[214] – which was also approved unanimously by the UN General Assembly.[215] It also welcomes the OEWG 2019/2021 report of 18 March 2021, which confirms this consensus.[216]

Switzerland views national positions of states as an important contribution to fleshing out the application of international law in cyberspace. This paper therefore gives an overview of Switzerland's position, but is neither exhaustive nor conclusive. Continuing intergovernmental exchange at multilateral level remains key in order to continue to clarify how international law is applicable to cyberspace in concrete terms. A definitive assessment of a cyber incident in terms of international law is only possible when the concrete circumstances are known. This means interpreting and applying the rules set out below in each individual case.

Of particular importance to the context of cybersecurity are namely the rules of international law described below.

---

[212] On Switzerland's work to establish an international regulatory framework in the digital space in general, refer to the Digital Foreign Policy Strategy (2021–24) and Annex 4 on the international rules and standards in particular (https://www.eda.admin.ch/dam/eda/en/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_EN.pdf).

[213] See Switzerland's Foreign Policy Strategy 2021–23, Objective 4.4 and Switzerland's Digital Foreign Policy Strategy 2021–24, Chapter 4.3.

[214] See Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013 Report (2013 Report, UN Doc. A/68/98, para. 19; 2015 Report (UN Doc. A/70/174), para. 24, para. 28 c).

[215] Resolution A/70/237.

[216] See Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021 report, para. 8, UN Doc. A/75/816.

I. General international law

1. Peaceful settlement of disputes

In accordance with Art. 2 para. 3 and Art. 33 of the UN Charter, disputes which may endanger the maintenance of international peace and security should be settled by peaceful means. This includes diplomatic proceedings, arbitration or recourse to the International Court of Justice (ICJ). As a neutral country with long-standing experience and engagement in the provision of good offices, Switzerland is committed to upholding this principle in cyberspace, emphasising the overriding aim of ensuring that cyberspace is used for peaceful purposes only. Switzerland therefore welcomes the UN GGE's 2015 report and the OEWG 2019/2021 report confirming the peaceful settlement of disputes as one of the UN Charter's central principles, which is also applicable to cyberspace. Consequently, disputes in cyberspace should also be settled by peaceful means, not with unilateral measures.

2. Sovereignty

Sovereignty is a foundational principle of international law. It refers to a state's jurisdiction to define, apply and enforce its own legal order, which in principle is limited to its territory. At interstate level however, sovereignty implies an independent and equal co-existence among states. Respect for and protection from interference with territorial integrity is a product of state sovereignty.[217] Accordingly, each state is obliged to respect the sovereignty of other states.[218] Sovereignty is a binding primary rule of international law. Violations of sovereignty are therefore considered internationally wrongful acts which, if attributable to the state itself, give rise to state responsibility.

State sovereignty is also applicable to cyberspace.[219] Owing to the special characteristics of cyberspace, which has no clear territorial boundaries, putting the principle of sovereignty into practice is a particular challenge. One major issue is who has jurisdiction over or access to digital data. In the cyber context, the key question is which states have legitimate control over digital data and are authorised to access that data – which may, depending on the circumstances, be stored on a different territory or may not be localised geographically. Conversely, in terms of interstate relations at cybersecurity level, the principle of sovereignty provides wide scope for protection against cyber operations. For example, state sovereignty protects information and communication technologies (ICT) infrastructure on a state's territory against unauthorised intrusion or material damage. This includes the computer networks, systems and software supported by the ICT infrastructure, regardless of whether the infrastructure is private or public.

Switzerland recognises that defining what constitutes a violation of the principle of sovereignty in cyberspace is particularly challenging and has yet to be clarified conclusively. It supports considering the following two criteria in such assessments: first, does the incident violate the state's territorial integrity and second, does it constitute interference with or usurpation of an inherently governmental function. A precise definition of these criteria is a question of interpretation and subject to debate. The current debate includes among other aspects i) incidents whereby the

[217] Arbitration award in the Island of Palmas case, 1928, p. 838; the Swiss Federal Constitution recognises state sovereignty under international law on the basis of independence, granting the state exclusive jurisdiction to make and enforce law within its territory (Art. 2 para. 1).

[218] Military and Paramilitary Activities in and against Nicaragua, ICJ Reports 1986, para. 292.

[219] UN GGE 2013 Report, para. 20; UN GGE 2015 Report, paras. 27 and 28 b).

functionality of infrastructure or related equipment has been damaged or limited, ii) cases where data has been altered or deleted, interfering with the fulfilment of inherently governmental functions such as providing social services, conducting elections and referendums, or collecting taxes, and iii) situations in which a state has sought to influence, disrupt or delay democratic decision-making processes in another state through the coordinated use of legal and illegal methods in cyberspace e.g. propaganda, disinformation and covert actions by intelligence services. The assessment of an individual case depends on the nature of the cyber incident and its repercussions.

3. Prohibition of intervention

The principle of non-intervention is the corollary of the sovereign equality of all states (Art. 2 para. 1 UN Charter) and is considered customary international law.[220] In this context, intervention is understood to be the direct or indirect interference by one sovereign state in the internal or external affairs of another using coercive measures. It covers those areas where the state has exclusive jurisdiction (known as domaine réservé). The non-intervention principle protects a state's ability to shape its own internal affairs (political, economic, social and cultural systems) as well as its foreign policy. An infringement of sovereignty and a prohibited intervention are not the same. The latter must be coercive in nature, i.e. through its intervention a state seeks to cause another to act (or refrain from acting) in a way it would not otherwise.[221] This means that the threshold for a breach of the non-intervention principle is significantly higher than that for a violation of state sovereignty.

The prohibition of intervention is also applicable to cyberspace. This means that in cyberspace, an unlawful act of interference by one state in the political or economic affairs of another may, in addition to constituting a violation of sovereignty, also breach the non-intervention principle under international law if the respective requirements are fulfilled.[222] The distinction between exerting influence, which is permissible, and coercion, which is not, must be determined on a case-by-case basis. This is particularly true of economic coercion, which could be the case if a company that is systemically relevant was paralysed through a cyber operation. An assessment of whether the operation can be deemed coercive in nature, and thereby be in breach of the non-intervention principle, can only be made on a case-by-case basis.

4. Prohibition on the use of force and the right of self-defence

One of the key founding principles of the UN Charter is the prohibition on the use of force (Art. 2 para. 4). There are only two exceptions: if the use of force is authorised by the UN Security Council (Art. 42) or if the strict conditions under which the right of self-defence may be exercised are fulfilled (Art. 51).

The prohibition on the use of force and the right of self-defence are also applicable to cyberspace. The right of self-defence may only be exercised if an armed attack occurs first. In accordance with ICJ case law, not every violation of the prohibition on the use of force constitutes an armed attack, but only its gravest form. In order to qualify, the scale and effect of the attack must reach a certain threshold of

[220] Friendly Relations Declaration, A/RES/2625 (XXV), 24 October 1970; Military and Paramilitary Activities in and against Nicaragua, ICJ reports 1986, para. 202.

[221] Military and Paramilitary Activities in and against Nicaragua, ICJ Reports 1986, para. 202.

[222] Explanatory notes to the Ordinance on Military Cyber Defence, SR 510.921.

gravity.[223] The ICJ has also determined that an armed attack does not necessarily have to involve kinetic military action or the use of weapons because the means by which an attack is perpetrated is not the decisive factor.[224] A state is permitted to exercise its right of self-defence in response to a cyber incident if the incident amounts in scale and effect to that of a kinetic operation in terms of inflicting death or serious injury to persons, or extensive material damage to objects. There are no binding quantitative or qualitative guidelines as to when the threshold of an armed attack in terms of scale and effect has been reached. Current discussions on how to define an armed attack in cyberspace are focusing on attacks on critical infrastructure (e.g. nuclear power plants, power grids) which reach the required threshold in terms of scale and effect i.e. serious injury to persons and/or extensive damage to objects.

The purpose of the UN Charter must guide the interpretation of the prohibition on the use of force and the right to exercise self-defence in the face of an armed attack. The Charter's objective is to maintain and, where necessary, restore international peace and security. Consequently, even if an armed attack occurs, a state is only permitted to undertake countermeasures that are necessary and proportionate in order to repel the attack. The right of self-defence only applies if the UN Security Council has not taken the necessary measures to maintain international peace and security (Art. 51 UN Charter). If the actions taken in self-defence exceed this framework, the state itself is in breach of the prohibition on the use of force. If the threshold for an armed attack has not been reached, states can have recourse to immediate and proportionate non-violent countermeasures (see section 6.2).

5. Neutrality

As a matter of principle, Switzerland considers the rights and obligations of neutral countries in international armed conflicts to be applicable to cyberspace as well.[225] If such an international armed conflict arises, a neutral country has a duty to prevent any infringements of its neutrality, such as the use of its territory by one of the conflicting parties. Parties to the conflict are obliged in turn to respect the territorial integrity of the neutral country. Therefore they may not conduct related cyber operations from installations that are either on the territory or under the exclusive control of the neutral country.[226] Parties to the conflict are also prohibited from taking control of a neutral country's computer systems in order to carry out such operations.[227]

Because of the global cross border nature of cyberspace, there are also limits to the rights and duties of a neutral country in terms of territoriality – airspace can be

[223] Military and Paramilitary Activities in and against Nicaragua, ICJ Reports 1986, para. 195.

[224] Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, para. 39.

[225] "The Court finds that as in the case of the principles of humanitarian law applicable in armed conflict, international law leaves no doubt that the principle of neutrality, whatever its content, which is of a fundamental character similar to that of the humanitarian principles and rules, is applicable (subject to the relevant provisions of the United Nations Charter), to an international armed conflict, whatever type of weapons might be used." Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, para 89.

[226] Art. 2 and Art. 3 Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (Hague V), 18 October 1907, SR 0.515.21; Art. 2 and Art. 5 Convention Concerning the Rights and Duties of Neutral Powers in Naval War (Hague XIII), 18 October 1907, SR 0.515.22.

[227] Art. 1 Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (Hague V), 18 October 1907, SR 0.515.21.

closed for certain flying objects, for example, but the same targeted approach cannot be used for data traffic on the internet. Another issue is that data are not only transmitted via terrestrial and cable channels but also via satellites located in outer space, which puts them outside the scope of application of the law of neutrality. Such factors must be taken into consideration when it comes to applying the rights and duties of neutral countries in cyberspace.

In principle, belligerent states are not permitted to damage the data networks of neutral countries when undertaking combat operations via their own computer networks. Neutral countries may not support conflicting parties with either troops or their own weapons. In terms of military cyber operations in connection with an international armed conflict, this means that a neutral country must prevent parties to the conflict from using its military-controlled systems or networks. In general, military networks are shielded and not publicly accessible.

6. State responsibility

The customary international rules on state responsibility are largely reflected in the draft articles issued by International Law Commission.[228] They are also applicable to cyber incidents. They provide that any state action in violation of international law shall entail the international responsibility of that state, upon which a claim for full reparation may be made. This only applies if the action can be legally attributed to the state and is deemed to constitute an internationally wrongful act, i.e. in violation of international law.

6.1 Attribution

Attribution of a cybersecurity incident refers to the identification of the perpetrator and describes a holistic, interdisciplinary process. This includes analysing the technical and legal aspects of the incident, factoring in the geopolitical context, and using the entire intelligence spectrum for the purpose of gathering information. Using this approach, a state can attribute a cyber incident to another state or a private actor, either publicly or not, and it can decide to take further political measures.

The process described above includes legal attribution, which ascertains whether a cyber incident can be legally attributed to a state and if that state can be held responsible under international law in accordance with the rules on state responsibility; it also concerns how the injured state may respond (known as countermeasures, see section 6.2). The conduct of any state organ or person exercising an inherently governmental function is always legally attributable to the state concerned.[229] If a cyber incident is carried out by a non-state actor, it can only be attributed to a state under certain conditions. In such cases, state responsibility only arises if the non-state actor acts on the instructions of a state, or under the direction or control of state organs.[230] If this requirement is met, the conduct constitutes an act by the state and is attributable to that state. The injured state is also permitted to take countermeasures (see section 6.2). If the required interstate dimension is lacking however, international law does not in principle permit countermeasures against another state.

---

[228] ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

[229] Art. 4 and Art. 5 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

[230] Art. 8 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

The decision to attribute conduct is at the discretion of the injured state and there is no obligation under international law to disclose the information leading to such a decision. Allegations of the organisation or implementation of an unlawful act against another state should however be substantiated.[231]

6.2 Countermeasures

A state may respond in different ways to unwelcome cyber activities carried out by another state.

Retorsion allows states to respond to such activities regardless of whether international law has been violated or not. It refers to unfriendly but lawful measures in response to unwelcome acts by another state. Typical examples of retorsion include refraining from signing a trade agreement that would benefit both parties, recalling an ambassador, or breaking off diplomatic relations as a last resort.

In cases where an act violates international law and can be legally attributed to a state, the injured state(s) may also take countermeasures in the form of reprisals, provided that the applicable rules governing state responsibility are observed.[232] Although reprisals are contrary to international law, they are justified in response to a prior breach of international law. However, such a countermeasure must not violate certain fundamental substantive obligations such as the prohibition on the use of force, fundamental human rights, most norms of international humanitarian law, peremptory norms (jus cogens) and the obligation to respect diplomatic and consular inviolability.[233] Military force, i.e. measures leading to loss of life and limb, are therefore prohibited.

Countermeasures must impose a (legal) disadvantage aimed at prompting the state concerned to cease its conduct that is in breach of international law and/or to make reparations. In principle, the responsible state can only impose countermeasures if it has first called for the violation(s) to cease and has announced what measures it is planning to take. Exceptions may be made for cyber operations requiring an immediate response in order for the injured state to enforce its rights and prevent further damage. Countermeasures must always be proportional, whatever the circumstances.

A countermeasure in response to a cyber incident does not necessarily have to take place in the cyber domain. In accordance with the rules governing state responsibility, other measures that aim to enforce the responsible state's compliance with its international obligations are also permissible. Cyber countermeasures do not have to directly target the computer system originally used to commit the incident in question; injured states are permitted to take other measures as long as they are aimed at the responsible state ceasing its conduct that is in breach of international law. This means that depending on the specific circumstances, it may be permissible under international law to use cyber countermeasures to block the computer system abroad originally used to commit the incident. Likewise, in some cases it may be permissible to compromise computer systems abroad even if they were not the original source of the incident.

---

[231] UN GGE 2015 Report, para. 28 f.

[232] ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001. Unless prohibited by international law, countermeasures are subject to strict conditions.

[233] Art. 50 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

In addition to countermeasures, the rules governing state responsibility also provide for special circumstances precluding the wrongfulness of conduct that would otherwise not be in conformity with the international obligations of the state concerned. For example, a state may be exempted from complying with such an obligation if it is the only way for it to safeguard its essential interests from grave and imminent peril. Therefore the narrowly defined exceptions provided for by the rules governing state responsibility may also apply in the context of cyber operations.[234]

6.3 Due diligence

The principle of due diligence has evolved over a long period of time. Switzerland views due diligence as part of customary international law and applicable to cyberspace. The ICJ describes the concept of due diligence as a standard of conduct meaning "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.[235] The doctrine of due diligence reflects fundamental principles of international law (including state sovereignty, equality, territorial integrity and non-interference).

The principle of due diligence is also applicable to cyberspace. Consequently, a state that is or should be aware of cyber incidents that violate the rights of another state is obliged to take all reasonable measures that are appropriate to stop or minimise the risks of such incidents. Due diligence is a variable standard and depends on the capacities and capabilities of a state as well as the particular circumstances of each case. Territorial states are obliged to use all reasonable means to prevent serious harm being caused to another state by activities taking place within their territory or in an area under their effective control. This makes due diligence an obligation of conduct, not of result. If the aforementioned conditions exist, the state in question is obliged under international law to close any loopholes immediately and assist in intercepting and tracing the incident.

Due diligence applies in particular to actions by private individuals that violate the rights of other states (e.g. hackers) and cannot be (clearly) attributed to the state in accordance with the rules of attribution (see section 6.1). If the aforementioned conditions exist and the state in question fails to fulfil due diligence requirements, the injured state may take countermeasures in accordance with the rules governing state responsibility in order to induce the responsible state to meet its obligations. Possible countermeasures outlined above may be taken both outside and inside the cyber domain. The responsible state may also be required to make reparations.[236]

7. Human rights

Human rights are a cornerstone of international law. They are enshrined in a number of treaties including the UN Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR). Fundamental human rights are also part of customary international law and can in part be categorised as *jus cogens*. Today, state obligations in respect of human rights have several dimensions.

---

[234] Chapter V, ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

[235] Corfu Channel case, ICJ Reports 1949, para. 44. Due diligence is both a general principle of international law, widely recognised as part of customary international law, and a prominent legal element in various international agreements where it has been enshrined, defined and further developed (e.g. environmental law, human rights law, IHL, global health law).

[236] Art. 31, ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

States must refrain from interfering with human rights (obligation to respect), protect individuals and groups against any such interference by third parties (obligation to protect) and take positive action to facilitate the enjoyment of basic human rights (obligation to fulfil).

Human rights also apply in the digital space and are a key pillar in the international regulatory framework for digitalisation. Individuals therefore have the same rights in the digital space as they do in physical space. This also applies to state security activities in cyberspace i.e. part of the digital space. Human rights obligations are equally binding upon states operating in cyberspace as in physical space. This also applies when the cyber operation in question is being carried out extraterritorially, to the extent that the States exercise their sovereign authority in doing so. If a cyber-related activity results in a violation of human rights, the victim will in principle have recourse to the enforcement mechanisms of the applicable domestic and international treaties in the same way as if the violation had been committed in physical space. Human rights monitoring bodies and tribunals can expand the scope and applicability of human rights in their practice.

A number of specific human rights may be particularly affected by cyber-related activities. An individual's right of access to information, right to privacy, or freedom of expression for example, could be restricted because of cyber operations or other cyber-related measures.

A state must be able to justify restricting these or other human rights in cyberspace based on the same rules that apply in physical space. In principle, any act of state interference requires an adequate legal basis. The state must also be able to demonstrate that in the balance of interests its actions are appropriate, necessary and reasonable in order to meet a legitimate objective.

Switzerland considers the applicability of human rights to cyberspace to be an unequivocal principle. However, new questions may arise when considering how this applies in individual cases. For example, if cyber-related activities are used to block access to social media, the question of freedom of expression may need to be clarified – at what point can this legally protected right be interfered with? Can the individual continue to exercise this right through alternative communication channels? To what extent are private actors also bound by human rights obligations? Human rights bodies need to develop their work in this field in order to ensure the application of human rights in cyberspace.

II. International humanitarian law

Switzerland considers international law to be applicable to cyberspace, which includes the application of IHL in the context of armed conflicts. Switzerland's foreign policy priorities include ensuring respect as well as strengthening and promoting IHL. Switzerland is well known for its neutrality, humanitarian tradition and role as depositary of the Geneva Convention. This position paper therefore addresses IHL issues in greater depth.

1. Applicability of IHL

IHL is applicable once an international or non-international armed conflict de facto exists. It is applicable in any armed conflict and to all parties to a conflict. IHL addresses the realities of war without considering the reasons for or the legality of the use of force. It does not deal with the legality of war, nor does it legitimise the use of

force between states.[237] The purpose of IHL is to regulate the conduct of hostilities and to protect victims of armed conflict, in particular by restricting the use of certain means and methods of warfare. The ICJ clearly stated that the established principles and rules of IHL apply to "all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future".[238]

This is applicable to cyberspace in the same way as for traditional and new operational spaces (outer space, airspace, land, maritime space, electromagnetic space, information space). IHL is therefore the main body of international law governing cyber operations that have a connection with an armed conflict. Implementing IHL effectively contributes to ensuring international security. Existing IHL, particularly its fundamental principles, places important limits on the execution of cyber operations in armed conflicts.

2. Fundamental IHL provisions regulating the conduct of hostilities

2.1 Principle concerning the means and methods of warfare

IHL prohibits or restricts means (weapons) and methods of warfare through general principles – regulating conduct or prohibiting certain effects – and specific rules addressing particular means and methods of warfare. As regards weapons, IHL distinguishes between the legality of a particular type of weapon (weapons law) and the legality of how it is used (law of targeting). The inherent characteristics of certain weapon categories entail that their use – in some or all circumstances – is unlawful *per se*. The admissibility of all other weapons depends on whether their use is in conformity with IHL.

This is also applicable to cyberspace. In fact, developing or using new means and methods of warfare must be in compliance with existing international law, particularly IHL. This is true even if a weapon is not covered by a specific norm and the treaty provisions governing the conduct of hostilities do not explicitly refer to new technologies. The customary rules of IHL apply equally to all means and methods of warfare, including in cyberspace. Indeed, it is a long standing principle that the right of parties to an armed conflict to choose methods or means of warfare is not unlimited.

2.2 Legality of a particular type of weapon

IHL stipulates that any means or method of warfare possessing one or more of the following characteristics is inherently unlawful if:

1) it is of a nature to cause superfluous injury or unnecessary suffering;

2) it is indiscriminate by nature, because it cannot be directed against a specific military objective or its effects cannot be limited as required by IHL;

3) it is intended, or may be expected, to cause widespread, long-term or severe damage to the natural environment; or

4) it is specifically prohibited by treaty or customary international law.

This is applicable to cyberspace and, therefore, to cyber means and methods of warfare.

---

[237] Any use of force between states is governed by the UN Charter and relevant customary international law (see above, section 1.4).

[238] Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, para. 86; "all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."

2.3 Legality of the manner in which the weapon is employed

With regard to the lawful use of cyber means and methods of warfare, the rules and principles governing the conduct of hostilities must be respected. Belligerents must in particular comply with the principles of distinction, proportionality and precaution by:

1) distinguishing between military objectives on the one hand, and civilians or civilian objects on the other hand and, in case of doubt, presume civilian status;

2) evaluating whether the incidental harm expected to be inflicted on the civilian population or civilian objects would be excessive in relation to the concrete and direct military advantage anticipated from that particular attack;

3) taking all feasible precautions to spare civilians and civilian objects.

This is also applicable in cyberspace, when using cyber means and methods of warfare. The aforementioned principles are applicable in particular to cyber operations that amount to an attack within the meaning of IHL i.e. acts of violence against the adversary, whether in offence or defence. What exactly constitutes a 'cyber attack' in an armed conflict has yet to be clarified. It encompasses at the very least cyber operations that are reasonably expected to cause, directly or indirectly, injury or death to persons, or physical damage or destruction to objects. The question, how exactly data is protected in the absence of such physical damage, remains a challenge. In practice, a responsible actor should generally be able to assess the potential impact of their actions and any resulting damage. As this estimation depends, amongst other things, largely on the information available at the time when decisions about an operation are taken, the obligation to take all precautionary measures practically possible to spare civilians and civilian objects plays a particularly important role in the use of cyber means and methods of warfare.

3. Other IHL provisions

Full compliance with IHL is not limited to the rules and principles governing the conduct of hostilities. There are other specific rules of IHL that must be respected, including when conducting military operations that do not qualify as an 'attack'. For example, certain categories of persons and objects are subject to special protection, such as medical, religious or humanitarian personnel and objects, which must be respected and protected in all circumstances.

This is also applicable to cyberspace. For cyber operations that are linked to any of these specially protected persons or objects, or to other activities governed by IHL, all of the relevant, specific rules must be observed.

4. Ensuring respect for IHL

States and parties to a conflict have an overarching obligation to “respect and ensure respect” for IHL “in all circumstances”. It is uncontested that preparatory measures must be taken to implement IHL and that its implementation needs to be supervised. This requires states and parties to a conflict, inter alia, to take measures to ensure that the development and use of means and methods of warfare fully comply with IHL, and to prevent outcomes that would be unlawful.

This is also applicable to cyberspace and the cyber means and methods of warfare. As with any other weapon, means or method of warfare, States have the positive obligation to determine, in their study, development, acquisition or adoption, whether their employment would, in some or all circumstances, violate existing international law.. In this regard, the obligation to assess the legality of a new weapon

as set out in Art. 36 of Additional Protocol I to the Geneva Conventions[239] is an important element to prevent or restrict the development and employment of new cyber weapons that would fail to meet in particular the obligations set out above.

***

Introduction

Dans les travaux du groupe d'experts gouvernementaux des Nations Unies chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale pour la période 2019-2021 (nommé ci-après « le GEG »), la dimension de politique de sécurité de l'espace numérique (cybersécurité) et les règles du droit international applicables dans ce contexte sont au premier rang des préoccupations des États[240]. La notion de cyberespace désigne la partie de l'espace numérique qui concerne la dimension de politique de sécurité. La prise de position de la Suisse traite d'abord de questions liées au droit international général, y compris les droits de l'homme (partie I), puis se concentre sur des questions relevant du droit international humanitaire (partie II).

La Suisse œuvre à bâtir et à garantir un cyberespace ouvert, libre, sûr et pacifique, et à promouvoir la reconnaissance, le respect et l'application du droit international dans cet espace[241]. Il est dans l'intérêt conjoint de tous les États de s'assurer que le cyberespace est régi selon les principes de l'état de droit et que l'utilisation qui en est faite est pacifique. Du point de vue de la Suisse, le droit international s'applique dans le cyberespace. La Suisse se félicite donc du consensus des GEGs précédents approuvé par les États membres de l'Assemblée générale des Nations Unies[242], selon lequel le droit international et en particulier la Charte des Nations Unies s'applique dans son intégralité dans le cyberespace[243]. Elle salue aussi la confirmation de ce consensus dans le rapport du 18 mars 2021[244] du groupe de travail à composition non limitée 2019-2021.

La Suisse considère que les positions nationales des États contribuent de manière significative à concrétiser davantage l'application du droit international dans le cyberespace. Sa prise de position présente un aperçu général de la question, qui n'est ni définitif ni complet. Outre les positions nationales, il est essentiel de continuer à clarifier la manière dont le droit international est applicable dans le cyberespace. L'application concrète du droit international dans le cyberespace passe aussi et surtout par des échanges étroits entre les États dans un cadre multilatéral. Comme

[239] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1), SR 0.518.521.

[240] Concernant l'engagement de la Suisse en faveur d'une réglementation internationale applicable à l'espace numérique en général, se référer à la stratégie de politique extérieure numérique 2021-2024 et en particulier à l'annexe 4. (https://www.eda.admin.ch/dam/eda/fr/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_FR.pdf).

[241] Objectif 4.4 de la stratégie de politique extérieure 2020-2023 et point 4.3 de la stratégie de politique extérieure numérique 2021-2024.

[242] Résolution A/70/237.

[243] Rapport 2013 (UNDOC A/68/98, par. 19) et rapport 2015 (UNDOC A/70/174, par. 24 et 28c) du groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

[244] Rapport 2021 (UNDOC A/75/816, par. 8) du groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

l'appréciation d'un cyberincident du point de vue du droit international n'est possible qu'à la lumière de ses circonstances concrètes, les règles du droit international évoquées ci-après doivent être interprétées et appliquées au cas par cas.

Les règles évoquées ci-après revêtent une importance particulière dans le contexte de la cybersécurité.

I. Droit international général

1. Règlement pacifique des différends

Conformément à l'art. 2, par. 3, et à l'art. 33 de la Charte des Nations Unies, les différends susceptibles de menacer le maintien de la paix et de la sécurité internationales doivent être réglés par des moyens pacifiques, comme une démarche diplomatique, ne arbitrage ou la saisine de la Cour internationale de Justice (CIJ). En tant que pays neutre avec un engagement et une expérience de longue date dans le domaine des bons offices, la Suisse s'investit afin que le principe du règlement pacifique des différends soit respecté dans le cyberespace également, soulignant ainsi que l'objectif premier est l'utilisation pacifique de cet espace. Elle salue donc le fait que le rapport 2015 du GEG et le rapport du groupe de travail à composition non limitée 2019-2021 ont confirmé que le règlement pacifique des différends, qui est l'un des principes centraux de la Charte des Nations Unies, s'applique également dans le cyberespace. Les différends dans le cyberespace doivent donc y être réglés par des moyens pacifiques et non par des mesures unilatérales.

2. Souveraineté

La souveraineté est un principe fondamental du droit international. D'une part, elle désigne la compétence des États à déterminer, appliquer et imposer leur ordre juridique dans les limites de leur territoire. D'autre part, elle implique que les États coexistent indépendamment les uns des autres et sur un pied d'égalité. Il découle du principe de souveraineté que chaque État a droit au respect de son intégrité territoriale et qu'il est protégé contre toute ingérence[245]. Chaque État doit de fait ne pas porter atteinte à la souveraineté d'un autre État[246]. De la souveraineté découle donc une règle primaire et contraignante du droit international, dont la violation constitue un acte contraire au droit international et engage la responsabilité de l'État auquel l'acte est attribué.

La souveraineté étatique s'applique également dans le cyberespace[247]. Comme ce dernier ne connaît pas de frontières territoriales clairement délimitées, la concrétisation du principe de souveraineté y représente un défi particulier. La question est notamment de savoir quels États exercent leur juridiction sur des données numériques ou ont accès à de telles données. Il convient également de s'intéresser au contrôle légitime des données numériques et au droit d'accéder à des données qui, selon les circonstances, peuvent être stockées sur un autre territoire ou dont la localisation géographique n'est pas possible. En matière de cybersécurité, le principe de souveraineté appliqué aux relations entre États permet toutefois d'identifier

[245] Affaire de l'île de Palmas (1928), p. 838. Sous la notion d'indépendance, l'art. 2, al. 1, de la Constitution fédérale de la Confédération suisse reconnaît à un État souverain au sens du droit international la compétence exclusive de définir et d'imposer le droit qui s'applique sur l'ensemble de son territoire.

[246] Activités militaires et paramilitaires au Nicaragua et contre celui-ci, arrêt, CIJ Recueil 1986, par. 292.

[247] Rapports 2013 (par. 20) et 2015 (par. 27 et 28b) du GEG.

différents domaines protégés contre les cyberopérations. Ainsi, la souveraineté protège l'infrastructure des technologies de l'information et de la communication (TIC) située sur le territoire de l'État souverain contre les intrusions non autorisées et les dégâts matériels. Sont donc protégés les réseaux informatiques, les systèmes et les logiciels qui composent les infrastructures TIC, qu'elles soient privées ou publiques.

La Suisse reconnaît que la concrétisation de ce qui constitue, dans le cyberespace, une violation d'un domaine protégé par la souveraineté étatique représente un défi particulier et n'est pas encore définitivement tranchée. De son point de vue, l'appréciation d'une telle violation doit notamment se fonder sur deux critères. Il convient de vérifier, d'une part, si l'incident viole l'intégrité territoriale d'un État et, d'autre part, s'il constitue une ingérence dans une fonction intrinsèque de cet État, voire une appropriation illicite de celle-ci. La compréhension exacte de ces critères est une question d'interprétation devant faire l'objet de discussions. Doivent notamment être discutés les cas dans lesquels le fonctionnement d'une infrastructure ou de son matériel connexe est altéré ou limité, les cas dans lesquels la modification ou la suppression de données entrave l'exécution de fonctions intrinsèques de l'État (p. ex. fourniture de prestations sociales, tenue d'élections et de votations, prélèvement de l'impôt) et les cas dans lesquels un État, par l'emploi coordonné de méthodes légales et illégales dans le cyberespace (p. ex. propagande, désinformation, opérations secrètes des services de renseignements), tente d'influencer, de perturber ou de retarder des processus décisionnels démocratiques dans un autre État. L'appréciation du cas individuel considéré dépend de la nature du cyberincident et de ses conséquences.

3. Non-intervention

Le principe de non-intervention découle du principe de l'égalité souveraine des États (art. 2, par. 1, de la Charte des Nations Unies) et fait partie intégrante du droit international coutumier [248]. Par intervention, on désigne l'ingérence directe ou indirecte d'un État, par des moyens de contrainte, dans les affaires intérieures ou extérieures d'un autre État. Sont visées les affaires relevant de la compétence exclusive de l'État (domaine réservé). Le domaine protégé par le principe de non-intervention englobe notamment les affaires intérieures d'un État que sont le choix de son système politique, économique, social et culturel et l'élaboration de sa politique extérieure. Contrairement à la violation de souveraineté, la violation du principe de non-intervention suppose un élément de contrainte : par son intervention, un État tente d'amener un autre État à agir (action ou omission) autrement qu'il ne l'aurait fait en l'absence de cette contrainte [249]. Ainsi, le seuil de violation du principe de non-intervention est sensiblement plus élevé que celui d'une violation de souveraineté.

Le principe de non-intervention s'applique également dans le cyberespace, où les actes d'un État peuvent constituer, si les conditions correspondantes sont réunies, outre une violation de souveraineté, une ingérence politique ou économique non autorisée dans les affaires intérieures ou extérieures d'un autre État. Ils peuvent

[248] Déclaration A/RES/2625 (XXV) du 24 octobre 1970 relative aux principes du droit international touchant les relations amicales et la coopération entre les États conformément à la Charte des Nations Unies ; Activités militaires et paramilitaires au Nicaragua et contre celui-ci, arrêt, CIJ Recueil 1986, par. 202.

[249] Activités militaires et paramilitaires au Nicaragua et contre celui-ci, arrêt, CIJ Recueil 1986, par. 202.

enfreindre ainsi le principe de non-intervention du droit international[250]. La limite entre l'action autorisée et la contrainte illicite doit être appréciée au cas par cas. Cela concerne en particulier la contrainte de nature économique, qui consiste par exemple à paralyser des entreprises d'importance systémique par l'intermédiaire d'une cyberopération. Un examen individuel est nécessaire afin d'établir si la cyberopération comprend un élément de contrainte et, donc, si elle porte atteinte au principe de non-intervention.

4. Interdiction du recours à la force et droit de légitime défense

L'un des principes fondamentaux de la Charte des Nations Unies est l'interdiction de recourir à la force (art. 2, par. 4). Des exceptions sont prévues si le Conseil de sécurité des Nations Unies estime nécessaire l'emploi de la force (art. 42) ou si les conditions strictes qui encadrent l'exercice du droit de légitime défense sont réunies (art. 51).

L'interdiction de recourir à la force et le droit de légitime défense s'appliquent également dans le cyberespace. Le droit de légitime défense ne peut être exercé que si l'État intéressé a été victime d'une agression armée. Selon la jurisprudence de la CIJ, toute violation de l'interdiction de recourir à la force ne constitue pas systématiquement une agression armée. Seules sont concernées les formes les plus graves d'emploi de la force, ce qui signifie que l'intensité et les effets de l'agression doivent atteindre une certaine gravité[251]. Selon cette même jurisprudence, une agression armée ne doit pas nécessairement être commise à l'aide de moyens ou d'armes cinétiques, car le moyen employé ne constitue pas un critère déterminant[252]. Un État peut exercer son droit de légitime défense en réaction à un cyberincident qui, au vu de la gravité des dégâts matériels ou des dommages aux personnes (blessées ou tuées), s'apparente dans son intensité et ses effets à une agression armée cinétique. Il n'existe pas de seuils quantitatifs et qualitatifs contraignants au-delà desquels l'intensité et les effets d'un emploi de la force qualifient une agression armée. Les discussions visant à caractériser une agression armée dans le cyberespace tendent à assimiler son intensité et ses effets à ceux d'une attaque contre une infrastructure critique (p. ex. une centrale nucléaire ou un réseau électrique) causant des dommages considérables aux personnes et/ou aux biens matériels.

En cas d'agression armée, l'interprétation de l'interdiction de recourir à la force et du droit de légitime défense doit tenir compte des objectifs de la Charte des Nations Unies – à savoir le maintien et, s'il y a lieu, le rétablissement de la paix et de la sécurité internationales. Même en cas d'agression armée, seuls sont autorisés les actes qui sont nécessaires et proportionnés pour se défendre contre l'agresseur. Le droit de légitime défense s'applique jusqu'à ce que le Conseil de sécurité de l'ONU ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales (art. 51 de la Charte des Nations Unies). Si la légitime défense sort de ce cadre, elle constitue elle-même un emploi illicite de la force. Si le seuil de l'agression armée n'est pas franchi, l'État intéressé a droit de prendre des contre-mesures non violentes immédiates et proportionnées (cf. point 6.2).

5. Neutralité

La Suisse estime que les droits et les devoirs d'un État neutre dans le contexte d'un conflit armé international sont en principe applicables dans le cyberespace

[250] Commentaires relatifs à l'ordonnance du 30 janvier 2019 sur la cyberdéfense militaire (OCMil, RS 510.921).

[251] Activités militaires et paramilitaires au Nicaragua et contre celui-ci, arrêt, CIJ Recueil 1986, par. 195.

[252] Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif, CIJ Recueil 1996, par. 39.

également[253]. L'État neutre a le devoir d'empêcher que l'utilisation de son territoire par une partie au conflit porte atteinte à sa neutralité, et les parties au conflit ont l'obligation de respecter son intégrité territoriale. Il s'ensuit que les parties au conflit ne sont pas autorisées à mener des cyberopérations en lien avec le conflit à partir d'installations situées sur le territoire d'un État neutre ou placées sous son contrôle exclusif[254]. Il leur est également interdit de prendre le contrôle de systèmes informatiques appartenant à l'État neutre pour conduire de telles opérations[255].

En raison de sa dimension transnationale globale, le cyberespace pose certaines limites aux droits et aux devoirs territoriaux des États neutres. Car s'il est possible d'interdire l'entrée d'un espace aérien à des aéronefs spécifiques, il est impossible de procéder de la même façon avec les données circulant sur Internet. D'autant que certaines données ne sont pas transmises uniquement par des câbles terrestres mais aussi par des satellites qui, parce qu'ils se situent dans l'espace, échappent au champ d'application du droit de la neutralité. Ces éléments doivent être pris en considération lorsque les droits et les devoirs des États neutres sont appliqués au cyberespace.

Il est fondamentalement interdit aux parties au conflit d'endommager les réseaux de données des pays neutres en raison des hostilités qu'elles mènent via les réseaux informatiques. Un État neutre n'est pas autorisé à soutenir les parties au conflit par l'envoi de troupes ou avec ses propres armes. Transposée aux cyberactivités militaires dans le contexte d'un conflit armé international, cette interdiction signifie qu'un pays neutre doit empêcher l'utilisation par les parties au conflit de ses propres systèmes et réseaux contrôlés militairement. En général, les réseaux militaires sont protégés et ne sont pas librement accessibles.

6. Responsabilité de l'État

Les règles sur la responsabilité de l'Etat reflètent essentiellement le droit international coutumier et sont largement reproduites dans le projet de la Commission du droit international[256]. Ces règles sont également applicables aux cyberincidents. Elles prévoient que tout fait internationalement illicite de l'État engage sa responsabilité internationale et donne droit à la réparation intégrale du préjudice. Cela ne s'applique que lorsqu'un comportement consistant en une action ou une omission est attribuable à l'État en vertu du droit international et constitue une violation d'une obligation internationale de l'État.

6.1 Attribution

[253] Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif, CIJ Recueil 1996, par. 89 : « La Cour estime que, comme dans le cas des principes du droit humanitaire applicable dans les conflits armés, le droit international ne laisse aucun doute quant au fait que le principe de neutralité – quel qu'en soit le contenu –, qui a un caractère fondamental analogue à celui des principes et règles humanitaires, s'applique (sous réserve des dispositions pertinentes de la Charte des Nations Unies) à tous les conflits armés internationaux, quel que soit le type d'arme utilisé. »

[254] Art. 2 et 3 de la Convention du 18 octobre 1907 concernant les droits et les devoirs des Puissances et des personnes neutres en cas de guerre sur terre (RS 0.515.21) et art. 2 et 5 de la Convention du 18 octobre 1907 concernant les droits et les devoirs des Puissances neutres en cas de guerre maritime (RS 0.515.22).

[255] Art. 1 de la Convention du 18 octobre 1907 concernant les droits et les devoirs des Puissances et des personnes neutres en cas de guerre sur terre (RS 0.515.21).

[256] Projet d'articles de la CDI sur la responsabilité de l'État pour fait internationalement illicite (août 2001).

L'attribution d'un cyberincident relevant de la politique de sécurité suppose d'identifier l'auteur de l'acte au moyen d'une procédure interdisciplinaire globale qui analyse les caractéristiques techniques et juridiques de l'incident, prend en considération le contexte géopolitique et utilise l'ensemble des activités de renseignements pour acquérir des informations. Sur cette base, l'État lésé par l'incident peut l'attribuer, publiquement ou non, à un autre État ou à un acteur privé et décider d'autres mesures politiques.

L'attribution du point de vue juridique est un volet de l'analyse décrite ci-dessus. Elle détermine si le cyberincident peut être juridiquement attribué à un autre État en vertu du droit international, si la responsabilité de cet autre État peut être engagée en application des règles énoncées par la CDI et comment l'État lésé est autorisé à y répondre dans les limites du droit international (cf. point 6.2 concernant les contre-mesures). Le comportement des organes de l'État et des personnes ou entités habilitées par le droit de cet État à exercer des prérogatives de puissance publique est considéré comme un fait de l'État d'après le droit international[257]. Un cyberincident causé par un acteur non-étatique peut également être attribué à l'État si cet acteur agit en fait sur les instructions d'un l'État, ou sous la direction ou le contrôle de celui-ci[258]. Ce comportement de l'acteur non-étatique doit alors être considéré comme un fait de l'État, ce qui autorise le pays lésé à prendre des contre-mesures (cf. point 6.2). En vertu du droit international, toute contre-mesure envers un autre État suppose toutefois que l'incident ait une dimension interétatique.

Les décisions découlant d'une telle attribution sont laissées à l'appréciation de l'État lésé. Le droit international n'impose aucunement à cet État de rendre publiques les informations l'ayant conduit à prendre ces décisions. Pour autant, toute accusation d'organiser et d'exécuter des actes illicites portée contre un État doit être étayée[259].

6.2 Contre-mesures

Un État lésé par les actes indésirables d'un autre État dans le cyberespace doit réagir de manière proportionnée et propre aux faits d'espèce.

L'État lésé est autorisé à user de rétorsion dans tous les cas, que l'acte indésirable constitue ou non une violation du droit international. Les mesures de rétorsion se définissent comme des mesures hostiles mais conformes au droit international, prises en réaction à la commission d'un acte indésirable par un autre État. Il s'agit ordinairement de refuser un accord commercial intéressant pour cet autre État, de rappeler son ambassadeur ou, en dernier recours, de rompre les relations diplomatiques avec cet État.

Si l'acte est juridiquement attribué et s'il est contraire au droit international, l'État lésé est autorisé à prendre des contre-mesures dans le respect des règles de la CDI définissant la responsabilité de l'État[260]. Les contre-mesures sont des mesures intrinsèquement contraires au droit international, qui se justifient toutefois lorsqu'un État réagit à une violation préalable du droit international par un autre État. Les contre-mesures ne peuvent néanmoins porter aucune atteinte à certaines obligations fondamentales telles que l'interdiction du recours à la force, la protection des droits

[257] Art. 4 et 5 du Projet d'articles de la CDI (août 2001).

[258] Art. 8 du Projet d'articles de la CDI (août 2001).

[259] Rapport 2015 du GEG (par. 28f).

[260] Projet d'articles de la CDI sur la responsabilité de l'État pour fait internationalement illicite (août 2001). Si tant est qu'elles ne soient pas interdites par le droit international, les contre-mesures sont assorties de conditions strictes.

de l'homme fondamentaux et l'obligation de respecter les normes du droit international humanitaire, les règles de ius cogens et le principe d'inviolabilité des missions diplomatiques et consulaires[261]. Il est donc exclu de faire usage de la force militaire, c'est-à-dire de prendre des mesures conduisant à la perte de vies humaines.

Les contre-mesures doivent toujours avoir pour but d'amener l'autre État, par l'imposition de sanctions (juridiques), à faire cesser son comportement violant le droit international et/ou à le réparer. En principe, elles ne peuvent être mises en œuvre que si elles ont été annoncées et si l'autre État a été préalablement enjoint de faire cesser son comportement. Dans le contexte des cyberopérations, il est possible de déroger à cette règle si l'État lésé doit prendre des contre-mesures immédiates afin de préserver ses droits et d'éviter d'autres dommages. Dans tous les cas, les contre-mesures doivent être proportionnelles au préjudice subi.

Les contre-mesures en réaction à un cyberincident ne doivent pas nécessairement être prises dans le domaine cyber : d'après les règles définissant la responsabilité de l'État, d'autres types de contre-mesure sont autorisés pour amener l'autre État à s'acquitter des obligations qui lui incombent en vertu du droit international. Si les contre-mesures interviennent dans le domaine cyber, elles ne doivent pas nécessairement viser le système informatique à l'origine de l'incident. D'autres cybermesures sont possibles pourvu qu'elles aient pour objectif d'amener l'autre État à faire cesser le comportement à l'origine de la violation du droit international. En fonction des circonstances concrètes de l'incident, le droit international autorise par exemple l'État lésé à bloquer l'exécution à l'étranger du système informatique incriminé ; dans certains cas individuels, il peut également l'autoriser à porter atteinte à des systèmes informatiques à l'étranger qui ne sont pas eux-mêmes à l'origine du cyberincident.

Conformément aux règles de la CDI sur la responsabilité de l'État, certaines circonstances spéciales peuvent exclure l'illicéité d'un fait de l'État non conforme à l'une de ses obligations internationales. Tel est notamment le cas si un tel fait de l'État constitue pour lui le seul moyen de protéger un intérêt essentiel contre un péril grave et imminent. Dans le cadre strict des exceptions prévues par les règles de la CDI, l'État peut déroger à des obligations internationales dans le contexte de cyberopérations également[262].

6.3 Devoir de diligence

Du point de vue de la Suisse, le devoir de diligence est un principe établi de longue date qui fait aujourd'hui partie intégrante du droit international coutumier et s'applique également dans le cyberespace. La CIJ décrit ce standard général de comportement comme « l'obligation, pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États[263] ». Le devoir de diligence est fidèle aux principes fondamentaux du droit international que sont

[261] Art. 50 du Projet d'articles de la CDI sur la responsabilité de l'État pour fait internationalement illicite (août 2001).

[262] Chap. V du Projet d'articles de la CDI sur la responsabilité de l'État pour fait internationalement illicite (août 2001).

[263] Affaire du détroit de Corfou, arrêt du 9 avril 1949, CIJ Recueil 1949, p. 22. Le devoir de diligence est d'une part un principe général du droit international reconnu comme coutumier et, d'autre part, une obligation ancrée, concrétisée et développée dans des traités internationaux relevant de différents domaines (p. ex. droit de l'environnement, droits de l'homme, droit international humanitaire, droit international de la santé).

notamment la souveraineté étatique, l'égalité, l'intégrité territoriale et la non-ingérence.

Ce principe s'applique aussi dans le cyberespace. Un État qui a ou devrait avoir connaissance de tels actes doit prendre toutes les mesures adéquates et raisonnables en son pouvoir pour faire cesser les cyberincidents contraires aux droits d'autres États ou pour minimiser leurs risques. Le devoir de diligence est un standard variable qui dépend des capacités et des possibilités de chaque État et des circonstances particulières de chaque cas. Il oblige l'État souverain à engager tous les moyens raisonnables à sa disposition pour empêcher que des activités menées sur son territoire ou dans une zone sous son contrôle effectif portent des préjudices graves à un autre État. En ce sens, le devoir de diligence est une obligation de comportement et non de résultat. Si les conditions énoncées sont réunies, le droit international oblige l'État responsable à combler immédiatement les failles de protection et à contribuer, par son aide, à lutter contre l'incident et à le tracer.

Le devoir de diligence concerne en particulier les situations dans lesquelles les droits d'autres États sont enfreints par des actes commis par des entités privées (p. ex. des groupes de hackers) qu'il n'est pas possible d'imputer clairement à l'État selon le principe d'attribution décrit au point 6.1. Si l'État responsable ne remplit pas le devoir de diligence exigé de lui en pareille situation, l'État lésé peut prendre des contre-mesures conformes aux règles de la CDI sur la responsabilité de l'État afin de l'amener à remplir ses obligations. Ces contre-mesures correspondent aux différentes options présentées ci-dessus et peuvent être prises dans le domaine cyber ou en dehors. L'État responsable peut par ailleurs être tenu de réparer le préjudice[264].

7. Droits de l'homme

Les droits de l'homme sont un pilier central du droit international. Ils sont garantis par différents traités internationaux dont le Pacte des Nations Unies relatif aux droits civils et politiques (Pacte II de l'ONU) et la Convention européenne des droits de l'homme (CEDH). Les droits de l'homme fondamentaux font également partie intégrante du droit international coutumier et constituent pour partie des normes impératives (*ius cogens*). Aujourd'hui, les droits de l'homme imposent aux États de s'abstenir de toute ingérence dans les droits de l'homme garantis aux individus (*obligation de respecter*), de protéger ces droits contre l'ingérence de tiers (*obligation de protéger*) et de prendre des mesures positives pour faciliter l'exercice de ces droits (*obligation de mettre en œuvre*).

Les droits de l'homme s'appliquent aussi dans l'espace numérique et sont un pilier central de la réglementation internationale en matière de numérisation. Quelles que soient les activités numériques considérées, les individus disposent des mêmes droits que dans l'espace physique. Cette règle s'applique également aux activités de politique sécuritaire que les États mènent dans le cyberespace, autrement dit dans un domaine partiel de l'espace numérique : lorsqu'ils opèrent dans le cyberespace, les États sont tenus de remplir leurs obligations en matière de droits de l'homme exactement comme dans l'espace physique – y compris lorsque ces cyberopérations sont extraterritoriales (dès lors que les États exercent ce faisant leur souveraineté). Si des cyberactivités aboutissent à une violation des droits de l'homme, les individus lésés disposent en principe des mêmes mécanismes d'exécution prévus par le droit international et applicables à l'échelle nationale que si la violation avait été commise dans l'espace physique. Dans ce domaine, la pratique des organes internationaux de

[264] Art. 31 du Projet d'articles de la CDI sur la responsabilité de l'État pour fait internationalement illicite (août 2001).

contrôle et juridictionnels est appelée à se développer en tenant compte de la portée et de l'applicabilité des droits de l'homme.

Certains droits de l'homme spécifiques peuvent être particulièrement concernés par des cyberopérations et autres mesures liées au domaine cyber, dans le sens où elles peuvent par exemple limiter le droit des individus à avoir accès à des informations, à préserver leur vie privée ou à exprimer librement leur opinion.

Les règles selon lesquelles un État peut justifier une restriction des droits de l'homme dans le cyberespace sont identiques aux règles applicables dans l'espace physique. Cela signifie que la restriction doit avoir une base légale suffisante et que l'État doit établir au moyen d'une pesée des intérêts que son ingérence est adaptée, nécessaire et raisonnable pour atteindre le but légitime visé.

S'il ne fait aucun doute pour la Suisse que les droits de l'homme s'exercent également dans le cyberespace, l'application de ce principe au cas par cas soulève toutefois de nouvelles questions. Prenons l'exemple d'une cyberactivité bloquant l'accès à des médias sociaux : s'agit-il d'une ingérence dans le bien public protégé qu'est la liberté d'expression ? Si oui, à partir de quel stade ? Le droit à la liberté d'expression peut-il s'exercer par d'autres moyens de communication ? Dans quelle mesure les acteurs privés sont-ils liés par les droits de l'homme ? Afin de garantir le respect des droits de l'homme dans le cyberespace, les instances compétentes en charge de cette thématique doivent encore mener des travaux complémentaires.

II. Droit international humanitaire

Du point de vue de la Suisse, le droit international est applicable au cyberespace, ce qui est également valable pour le droit international humanitaire (DIH) dans le contexte de conflits armés. Le respect, le renforcement et la promotion du DIH sont des priorités de la politique extérieure de la Suisse – pays qui se caractérise par sa neutralité, sa tradition humanitaire et son statut d'État dépositaire des Conventions de Genève. C'est pour cette raison que la Suisse examine plus en profondeur la question du DIH dans la présente prise de position.

1. Applicabilité du DIH

Le DIH est applicable lorsqu'un conflit armé, international ou non-international, existe de fait. Il s'applique à tous les types de conflits armés et à l'ensemble des parties au conflit. Il s'intéresse aux réalités des conflits, indépendamment des motifs ou de la licéité du recours à la force. Il n'apporte aucune réponse à la question de la licéité des conflits et ne légitime aucunement l'emploi de la force entre États[265]. Le DIH a pour but de réglementer la conduite des hostilités et de protéger les victimes de conflits armés, principalement en limitant l'utilisation des méthodes et moyens de guerre. Selon la CIJ, les principes et règles établis du DIH s'appliquent « à toutes les formes de guerre et à toutes les armes, celles du passé, comme celles du présent et de l'avenir [266]».

Cela est valable pour le cyberespace de la même manière que pour les théâtres d'opérations conventionnels ou nouveaux (p. ex. espace, air, sol, espace maritime, espace électromagnétique, espace de l'information). Ainsi, le DIH est la principale branche du droit international réglementant les cyberopérations en situation de conflits armés. Sa

[265] Tout recours à la force entre États est réglementé par la Charte des Nations Unies et par le droit international coutumier applicable (cf. point 4 ci-dessus).

[266] Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif, CIJ Recueil 1996, par. 86.

mise en œuvre effective contribue à garantir la sécurité internationale. Le DIH existant, et en particulier ses principes fondamentaux, posent d'importantes limites à l'exécution de cyberopérations dans le contexte de conflits armés.

2. Dispositions fondamentales du DIH réglementant la conduite des hostilités

2.1 Principe relatif aux méthodes et moyens de guerre

Le DIH restreint ou interdit les méthodes et moyens (armes) de guerre en fixant d'une part des principes généraux qui réglementent les comportements et prohibent la production de certains effets et, d'autre part, des règles spécifiques qui s'appliquent à des méthodes et moyens de guerre en particulier. S'agissant des armes, le DIH fait une distinction entre la licéité de l'arme elle-même (*weapons law*) et la licéité liée à son emploi (*law of targeting*). Les caractéristiques inhérentes à certaines catégories d'armes impliquent que leur utilisation - dans certaines ou toutes les circonstances - est illégale en soi. Pour l'ensemble des autres armes, la licéité de l'emploi dépend de sa conformité avec le DIH.

Cela s'applique également dans le cyberespace. En effet, le développement et l'emploi de nouvelles méthodes et moyens de guerre doivent respecter le droit international en vigueur, et en particulier le DIH. Il en va également ainsi si l'arme n'est pas couverte par une norme spécifique et si les dispositions conventionnelles réglementant la conduite des hostilités ne se rapportent pas expressément aux nouvelles technologies. Les règles coutumières du DIH sont applicables de manière égale à l'ensemble des méthodes et moyens de guerre, donc également dans le cyberespace. En effet, selon un principe établi de longue date, le droit des parties à un conflit armé de choisir les méthodes ou moyens de guerre n'est pas illimité.

2.2 Licéité d'un type particulier d'armes

En application du DIH, les méthodes et moyens de guerre qui présentent une ou plusieurs des caractéristiques suivantes sont intrinsèquement illicites :

la méthode ou le moyen de guerre :

(1) est de nature à causer des maux superflus ;

(2) produit des effets indiscriminés parce qu'il ne peut pas être dirigé vers un objectif militaire déterminé ou parce que ses effets ne peuvent pas être limités de la manière prescrite par le DIH ;

(3) est conçu pour causer, ou dont on peut attendre qu'il causera, des dommages étendus, durables et graves à l'environnement naturel ; *ou*

(4) est expressément interdit par le droit conventionnel ou le droit coutumier.

Cela s'applique également dans le cyberespace et donc aux méthodes et moyens de guerre relevant du domaine cyber.

2.3 Licéité de l'emploi des méthodes et moyens de guerre

En ce qui concerne l'utilisation licite des moyens et méthodes de guerre cybernétiques, les règles et principes régissant la conduite des hostilités doivent être respectés. Cela signifie que les belligérants doivent respecter en particulier les principes de distinction, de proportionnalité et de précaution, c'est-à-dire :

(1) distinguer les objectifs militaires, d'une part, et la population civile ou les biens civils, d'autre part, en présumant du caractère civil en cas de doute ;

(2) évaluer si les dommages potentiels pour la population civile ou les biens civils ne seraient pas disproportionnés par rapport à l'avantage militaire direct et concret attendu ;

(3) prendre toutes les mesures de précaution pratiquement possibles afin que les personnes et les biens protégés soient épargnés par les conséquences des opérations militaires.

Cela s'applique également dans le cyberespace lorsque des méthodes et moyens de guerre relevant du domaine cyber sont utilisés. Ces principes s'appliquent en particulier aux cyberopérations assimilables à une attaque au sens du DIH, c'est-à-dire aux actes de violence contre l'adversaire, que ces actes soient offensifs ou défensifs. Ce qui constitue une « attaque cyber » dans le contexte d'un conflit armé reste toutefois à clarifier. Cela comprend pour le moins des cyberopérations dont on peut raisonnablement s'attendre qu'elles auront pour effet direct ou indirect de blesser voire de tuer des personnes et/ou d'endommager physiquement voire de détruire des biens. En l'absence de tels dégâts physiques, un des défis qui demeure est de savoir dans quelle mesure les données sont protégées. Dans la pratique, un acteur conscient de ses responsabilités devrait pouvoir estimer les effets possibles de ses actions et les dégâts y relatifs. Mais comme cette estimation dépend notamment des informations disponibles au moment de décider d'une opération, l'obligation de prendre toutes les mesures de précaution pratiquement possibles pour épargner la population et les biens civils avant d'employer des méthodes et des moyens de guerre dans le domaine cyber joue de fait un rôle particulièrement important.

3. Autres dispositions du DIH

L'obligation de respecter pleinement le DIH ne se limite pas aux règles et aux principes régissant la conduite des hostilités. Il existe d'autres règles spécifiques du DIH qui doivent être respectées, y compris lors d'opérations militaires ne constituant pas une « attaque ». C'est notamment le cas des personnes et des biens bénéficiant d'une protection spéciale. Par exemple, le personnel médical, religieux ou humanitaire et les biens y associés doivent être respectés et protégés en toutes circonstances.

Cela s'applique également dans le cyberespace. Les cyberopérations affectant des catégories de personnes ou d'objets particulièrement protégées ou d'autres aspects réglementés par le DIH doivent tenir compte de toutes les règles spécifiques applicables.

4. Garantie du respect du DIH

Les États et les parties à un conflit ont l'obligation fondamentale de « respecter et faire respecter » le DIH en toutes circonstances. Il est incontesté que des mesures préparatoires doivent être prises pour permettre la mise en œuvre du DIH et que sa mise en œuvre doit être surveillée. Ainsi, les États et les parties à un conflit doivent notamment prendre des mesures afin de s'assurer que le développement et l'emploi de méthodes et de moyens de guerre respectent strictement le DIH et pour éviter toute conséquence contraire au droit.

Cela s'applique également au cyberespace et donc aux méthodes et moyens de guerre relevant du domaine cyber. Comme pour toute autre arme, méthode ou moyens de guerre, les États ont l'obligation positive, lorsqu'ils les étudient, mettent au point, acquièrent ou adoptent, de déterminer si leur emploi serait susceptible, dans certaines ou en toutes circonstances, de contrevenir au droit international existant. Dans cette optique, l'obligation de déterminer la conformité des nouvelles armes avec le DIH conformément à l'art. 36 du Protocole additionnel aux Conventions de Genève[267] constitue un élément important pour empêcher ou limiter le développement et l'emploi de nouvelles cyberarmes qui, en particulier, ne rempliraient pas les conditions précitées.

[267] Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), RS 0.518.521.

United Kingdom of Great Britain and Northern Ireland

[Original: Arabic, Chinese, English, French, Russian and Spanish]

مقدمة

1. القانون الدولي له دور أساسي في الحفاظ على الأمن والاستقرار في الفضاء الإلكتروني، وهو ينطبق على سلوك الدول في الفضاء الإلكتروني تماما كما ينطبق على سلوكها في مجالات أخرى. وتطبيق القانون الدولي على سلوك الدول في الفضاء الإلكتروني مُعتمد بوضوح من قبل المجتمع الدولي. وفي تقرير الفريق العامل مفتوح العضوية الصادر مؤخرا في 2021، عاودت الدول تأكيد فهمها (كما هو مبين بالفعل في تقريريّ فريق الخبراء الحكوميين في 2013 و2015) بأن "أحكام القانون الدولي، لا سيما ميثاق الأمم المتحدة، قابلة للتطبيق وضرورية فيما يتعلق بالمحافظة على السلام والاستقرار، وتعزيز توفير بيئة مفتوحة وآمنة ومستقرة وميسرة وسلمية في مجال تكنولوجيا المعلومات والاتصالات".

بالتالي ترحب المملكة المتحدة بالمبادرة الحالية التي تحث الدول على تقديم بيانات تُرفق بتقرير فريق الخبراء الحكوميين، وتوضح مواقفها الوطنية تجاه انطباق القانون الدولي على السلوك في الفضاء الإلكتروني. من شأن ذلك أن يساعد الدول في تعزيز فهم أفضل للقانون الدولي وتطويره، وأن ييسر شفافية، وفهما مشتركا، أكبر بشأن ما يُعتبر سلوكا مقبولا في الفضاء الإلكتروني. فكلما زاد الوضوح حول حدود السلوك القانوني، كلما قل خطر سوء التقدير، وكلما كانت العواقب أوضح بالنسبة لمن يتجاوز هذه الحدود. الغرض من هذا البيان هو أن يكون مساهمة في هذه المبادرة، وأن يعرض بإيجاز، وليس بشكل مستفيض، موقف المملكة المتحدة تجاه عدد من المسائل المعينة المتعلقة بكيفية انطباق القانون الدولي على سلوك الدول في الفضاء الإلكتروني.

المملكة المتحدة ملتزمة بأن يكون الفضاء الإلكتروني مجانيا ومفتوحا وسلميا وآمنا. واستخدام الفضاء الإلكتروني هو في صالح الدول والمجتمع الدولي ككل، ولدى الدول الحق في ممارسة قدراتها الإلكترونية، رهنا بالقيود التي يفرضها القانون الدولي. وبينما لا يوجد تعريف دولي متفق عليه لمصطلح "الفضاء الإلكتروني"، فإنه مستخدم في هذا البيان للإشارة إلى نطاق الأفعال والأداء بالاستعانة بشبكة مترابطة من البنية التحتية لتكنولوجيا المعلومات، والتي تشمل الإنترنت، وشبكات الاتصالات المتصلة بالإنترنت، وأنظمة الحاسوب، والأجهزة المتصلة بالإنترنت.[268] ومصطلح "إلكتروني" مستخدم في هذا البيان للإشارة إلى الأفعال التي تستعين بالبنية التحتية لتكنولوجيا المعلومات.

ميثاق الأمم المتحدة

ميثاق الأمم المتحدة ينطبق على سلوك الدول في الفضاء الإلكتروني، تماما كما ينطبق على سلوكها في مجالات أخرى.

المادة 2(4) من ميثاق الأمم المتحدة تمنع استخدام القوة أو التهديد باستخدامها لتهديد سلامة أراضي دولة أو استقلالها السياسي، أو استخدامها على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة. وبناء على الحقائق والظروف المحيطة بكل حالة، يمكن أن يشكل سلوك الدولة في الفضاء الخارجي استخداما للقوة أو تهديدا باستخدامها إن كان للعمل الواقع أو الذي تهدد بالقيام به آثار، أو كان يمكن أن تكون له آثار، الفعل بالاستعانة بالسبل التقليدية (*kinetic*). والظروف التي يكون فيها استخدام القوة أو التهديد باستخدامها ليس ممنوعا بموجب القانون الدولي هي نفسها سواء كان العمل تقليديا أو إلكترونيا.

العملية التي تُنفذ بسبل إلكترونية يمكن أن تعتبر اعتداء مسلحا، وتستدعي ممارسة الحق الطبيعي للدفاع عن النفس بشكل فردي أو جماعي، كما هو مبين في المادة 51 من ميثاق الأمم المتحدة، حين يكون نطاق وأثر العملية مساويا لأثر ونطاق هجوم مسلح تقليدي. وعوامل النظر في نطاق وأثر أي

[268] يستند هذا التعريف بمعناه الواسع إلى تعريف الفضاء الإلكتروني كما ورد في الاستراتيجية الوطنية لأمن المعلوماتية 2016-2021 الصادرة عن الحكومة البريطانية، والتي يمكن قراءتها على هذا الرابط https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643427/Arabic_translation_-_National_Cyber_Security_Strategy_2016.pdf والتي تعرف الفضاء الإلكتروني بأنه "شبكة مترابطة من البنية التحتية لتكنولوجيا المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والأجهزة المتصلة بالإنترنت، إلى جانب المعالِجات وأجهزة التحكم المرتبطة بها. كما يمكن أن يشير المصطلح إلى عالم أو نطاق افتراضي كظاهرة مجربة أو مفهوم مجرّد".

اعتداء قد تشمل (فعليا أو بشكل متوقع) الدمار المادي للممتلكات أو التسبب في وقوع إصابات أو وفاة. وممارسة الحق الطبيعي بالدفاع عن النفس ضد هجوم مسلح وشيك أو مستمر، سواء كان هجوما تقليديا أو إلكترونيا، يمكن بحد ذاتها أن تكون بالسبل التقليدية أو بسبل إلكترونية، ويجب أن يستوفي دائما متطلبات الضرورة والتناسب. ومسألة ممارسة أو عدم ممارسة الحق الطبيعي بالدفاع عن النفس تُدرس بعناية دائما مع أخذ جميع الظروف بعين الاعتبار.

المادة 2(3) وأحكام الفصل السادس من الميثاق بشأن حل النزاعات سلمياً يمكن أن تنطبق كذلك على نشاط الدول في الفضاء الإلكتروني. وبالتالي، وبموجب المادة 33(1)، يلزم على الدول الأطراف في أي نزاع إلكتروني دولي من المرجح أن يهدد استمراره السلام والأمن الدوليين السعي إلى تسوية ذلك الخلاف بالسبل السلمية كما هو مبين في المادة 33 من الميثاق: التفاوض والتحقيق والوساطة والتوفيق والتحكيم والتسوية القضائية، أو اللجوء إلى هيئات أو ترتيبات إقليمية أو غيرها من السبل السلمية التي يقع عليها الاختيار.

السيادة وعدم التدخل

بالنسبة لفعل يكون دون عتبة استخدام القوة أو التهديد باستخدامها، فإن قاعدة القانون الدولي العرفي بشأن منع التدخل في الشؤون الداخلية للدول تنطبق على عمليات الدول في الفضاء الإلكتروني مثلما تنطبق على نشاطاتها الأخرى. وكما يتضح من حكم محكمة العدل الدولية في قضية نيكاراغوا، الغرض من قاعدة عدم التدخل هو توفير ضمان لجميع الدول بعدم تعرض أي دولة لتدخل خارجي قسري في مسائل تؤثر على صلاحياتها التي تشكل صميم سيادة الدولة، مثل حرية اختيار نظامها السياسي والاجتماعي والاقتصادي والثقافي.[269]

مثلما أشارت المملكة المتحدة من قبل، الحدود الدقيقة لهذه القاعدة، بينما أنها لا تزال موضوع نقاش مستمر، توفر أساسا واضحا وراسخا في القانون الدولي لتقييم مدى قانونية سلوك الدول. وبالتالي فإن اللجوء إلى عمليات إلكترونية معادية للتلاعب بالنظام الانتخابي في دولة أخرى لتغيير نتائج الانتخابات، أو لتقويض استقرار النظام المالي في دولة أخرى، أو للقيام بأفعال تستهدف الخدمات الطبية الأساسية في دولة أخرى يمكن أن تعتبر جميعها، تبعا للظروف، انتهاكا لمبدأ منع التدخل بموجب ما ينص عليه القانون الدولي.

رأت محكمة الجنايات الدولية بأن التدخل الممنوع هو التدخل الذي يكون له أثر على مسائل يُسمح لكل دولة، من منطلق مبدأ السيادة، أن تتخذ بشأنها قرارات بكل حُرية. والسيادة، كمبدأ عام، تعتبر مفهوماً أساسياً في القانون الدولي. والمملكة المتحدة تستذكر بأن أي منع لأنشطة الدول، سواء كان ذلك يتعلق بالفضاء الخارجي أو مسائل أخرى، يجب أن تكون له أسس واضحة إما في القانون الدولي العرفي أو في اتفاقية ملزمة للدول المعنية. والمملكة المتحدة لا ترى بأن المفهوم العام للسيادة بحد ذاته يعطي أساسا كافيا أو واضحا لاستنباط قاعدة معينة، أو لمنع إضافي لسلوك إلكتروني يتجاوز مبدأ عدم التدخل المشار إليه أعلاه. وفي نفس الوقت، تشير المملكة المتحدة إلى ضرورة ألا يؤدي الاختلاف في وجهات النظر حول هذه المسائل إلى منع الدول من تقييم ما إن كانت أوضاع معينة ترقى إلى كونها أفعالا غير مشروعة دوليا، والوصول إلى استنتاجات مشتركة حول تلك المسائل.

مسؤولية الدولة وعزو الأفعال

تكون الدولة مسؤولة بموجب القانون الدولي عن النشاط الإلكتروني الذي يُعزى إليها بموجب قواعد مسؤولية الدولة. وبالتالي فإن مسؤولية دولة ما عن أنشطة نابعة من أراضيها، بما في ذلك الأنشطة المرتبطة بالفضاء الإلكتروني، تتحدد بموجب قواعد القانون الدولي بشأن مسؤولية الدولة. وإلى

[269] العمليات العسكرية وشبه العسكرية في نيكاراغوا وضدها (نيكاراغوا ضد الولايات المتحدة الأمريكية)، أساس الدعوى والحكم بها، تقارير محكمة الجنايات الدولية في 1986 في الفقرة 205: في هذا الصدد ترى [المحكمة] بأن، بالنظر إلى الصيغ المقبولة عموما، يمنع المبدأ جميع الدول أو جماعات الدول من التدخل بشكل مباشر أو غير مباشر في الشؤون الداخلية أو الخارجية لدول أخرى. وتبعا لذلك، فإن التدخل الممنوع هو أي تدخل يؤثر على مسائل يُسمح لكل دولة، استنادا إلى مبدأ السيادة، أن تتخذ قرارات بشأنها بكل حرية. من بين هذه المسائل اختيار النظام السياسي والاقتصادي والاجتماعي والثقافي، ووضع السياسة الخارجية. التدخل يكون غير مشروع حين يعتمد على وسائل الإكراه بشأن هذه الخيارات، والتي يجب أن تظل خيارات حرة. وعنصر الإكراه، الذي يحدد، وبالتأكيد يشكل جوهر، التدخل الممنوع واضح بشكل خاص في قضية التدخل باستخدام القوة، سواء بشكل مباشر كما في العمل العسكري، أو بشكل غير مباشر بصورة دعم نشاط تخريبي أو نشاط جماعات مسلحة في دولة أخرى."

جانب مسؤوليتها عن أفعالها وأفعال وكلائها، تتحمل الدولة المسؤولية كذلك، بموجب القانون الدولي، على سبيل المثال حين يتصرف شخص أو جماعة من الأشخاص بناء على تعليماتها أو بموجب توجيهاتها أو تحت سيطرتها.

المعيار 13(ج) من معايير فريق الخبراء الحكوميين التابع للأمم المتحدة ينص على أنه لا يجوز للدول أن تسمح عن سابق علم باستغلال أراضيها للقيام بأفعال غير مشروعة دوليا باستخدام تكنولوجيا المعلومات والاتصالات. ويعطي هذا المعيار توجيهات بشأن ما يمكن أن يكون سلوكا مناسبا متوقعا من الدولة. تدرك المملكة المتحدة أهمية أن تتخذ الدول خطوات عملية مناسبة ومتاحة بشكل معقول ضمن قدراتها لمعالجة أنشطة تدرك بأنها ضارة لأجل تعزيز استقرار الفضاء الإلكتروني لما هو في مصلحة جميع الدول. لكن كون الدول قد أشارت إلى هذا المعيار على أنه غير ملزم إنما هي دلالة على عدم وجود ممارسات كافية من الدول لترسيخ قاعدة مراعاة "العناية الواجبة" المحددة في القانون الدولي العرفي التي تنطبق على الأنشطة في الفضاء الإلكتروني.

مصطلح "العزو" يُستخدم في مجال الفضاء الإلكتروني بدلالته القانونية وغير القانونية على حد سواء. حيث يشير في دلالته القانونية إلى تحديد المسؤولين عن عمل دولي غير مشروع. كما يُستخدم بدلالته غير القانونية إشارة إلى تحديد الفاعلين (بما في ذلك الفاعلين من غير الدول) الذين قاموا بفعل إلكتروني يمكن أن يُعتبر فعلا معاديا أو خبيثا لكنه لا ينطوي بالضرورة على عمل دولي غير مشروع.

بالنسبة للمملكة المتحدة، هناك جوانب فنية ودبلوماسية تؤخذ في عين الاعتبار لتحديد ما إن كانت سوف تعزو علنيا مثل هذه الأنشطة في الفضاء الخارجي للدولة المسؤولة عنها. وقرار ما إن كانت سوف تدلي ببيان يعزو الفعل علنا هي مسألة تتعلق بالسياسة. حيث يُنظر إلى كل حالة بناء على وقائعها. المملكة المتحدة تعزو فعلا ما علنا من منطلق التزامها بالوضوح وبضمان الاستقرار في الفضاء الخارجي أو حينما يكون من مصلحتها فعل ذلك.

مهما كانت طبيعة عزو الفعل، ليس هناك التزام قانوني عام يتطلب من الدولة أن تكشف علنا أي معلومات لديها استندت إليها في قرارها لعزو الفعل.

التدابير المضادة

ربما يُلجأ إلى اتخاذ تدابير مضادة ردا على فعل غير مشروع دولياً، بموجب القانون الدولي، تتعلق بأنشطة الدول في الفضاء الإلكتروني تماما كالتدابير المتخذة بشأن أنشطتها الأخرى. ذلك يشمل اللجوء إلى تدابير مضادة ضد دولة تشكل أنشطتها الإلكترونية أفعالا غير مشروعة دوليا، واتخاذ تدابير مضادة من خلال عمليات إلكترونية. التدابير المضادة لا يلزم أن تكون بالضرورة متماثلة: فحينما يكون الفعل غير المشروع دوليا بحد ذاته ليس نشاطا إلكترونيا، يمكن مع ذلك أن ينطوي الرد عليه على اتخاذ تدابير مضادة إلكترونية (والعكس بالعكس).

يمكن للدولة المتضررة أن تتخذ تدابير مضادة فقط ضد الدولة المسؤولة عن الفعل غير المشروع دوليا لحمل تلك الدولة على الامتثال لالتزاماتها. ويجب أن تكون أي تدابير تتخذها متناسبة مع الضرر الذي تعرضت له. وهذه التدابير المضادة يجب أن تكون متماشية مع الشروط والقيود المحددة في القانون الدولي، وألا تخالف بشكل خاص مبدأ منع استخدام القوة أو التهديد باستخدامها، ويجب أن تكون ضرورية ومتناسبة مع غرض حمل الدولة المسؤولة على الامتثال لالتزاماتها، ولا تخالف أي معيار آخر قطعي في القانون الدولي.

انطباق القانون الدولي على اللجوء إلى تدابير مضادة في الفضاء الإلكتروني يجب أن يأخذ في عين الاعتبار طبيعة الأنشطة الإلكترونية، والتي يمكن أن تبدأ وتتوقف فورا أو في غضون إطار زمني قصير. في مثل تلك الحالات، ربما يشكل نمطٌ أوسع من أنشطة إلكترونية مجتمعة فعلا غير مشروع دوليا يبرر الرد عليه.

المملكة المتحدة لا ترى بأن الدول التي تتخذ تدابير مضادة ملزمة قانونيا بإعطاء إشعار مسبق (بما في ذلك مطالبة الدولة المسؤولة عن الفعل غير المشروع دوليا بالامتثال للقانون الدولي) في جميع الحالات. حيث إن إعطاء إشعار مسبق قد لا يكون واجبا قانونيا عند الرد بتدابير مضادة على اختراق إلكتروني سري، أو لدى الاضطرار إلى اللجوء إلى تدابير مضادة تعتمد بحد ذاتها على قدرات إلكترونية سرية. ففي مثل هذه الحالات، إعطاء إشعار مسبق يمكن أن يكشف عن قدرات شديدة الحساسية ويضر بفعالية التدابير المضادة المعنية. لكن أي قرار للجوء إلى اتخاذ تدابير

مضادة دون إعطاء إشعار مسبق يجب أن يكون قرارا ضروريا ومتناسبا مع غرض حمل الدولة المعتدية على الامتثال في تلك الظروف.

القانون الدولي لحقوق الإنسان

التزامات الدول بحقوق الإنسان تنطبق على أنشطتها في الفضاء الإلكتروني مثلما تنطبق على أفعالها الأخرى. والمملكة المتحدة مستمرة بدعم الرأي المشار إليه في قرار مجلس حقوق الإنسان 8/20 بأن "الحقوق التي يتمتع بها الناس في الواقع يجب أن تكون محمية كذلك أثناء استخدامهم للإنترنت...". يقع على عاتق الدول واجب التصرف بموجب قوانين حقوق الإنسان الدولية المعمول بها، بما فيها [القانون الدولي العرفي]، والأعراف الدولية التي هي طرف فيها مثل العهد الدولي الخاص بالحقوق المدنية والسياسية، وغيرها من اتفاقيات الأمم المتحدة، وآليات إقليمية كالاتفاقية الأوروبية لحقوق الإنسان.

احترام الدول لالتزاماتها بحقوق الإنسان فيما يتعلق بأنشطتها في الفضاء الإلكتروني ضروري لضمان وجود بيئة مفتوحة وآمنة ومستقرة ومتاحة للجميع وسلمية، وربما يكون لحقوق معينة صلة خاصة بأنشطة الدول في الفضاء الإلكتروني، بما في ذلك حق عدم التعرض لتدخل قسري أو غير قانوني بخصوصية الفرد أو عائلته أو بيته أو مراسلاته، وحق حرية الفكر والضمير والدين، وحق حرية التعبير عن الرأي.

القانون الدولي الإنساني

ينطبق القانون الدولي الإنساني على العمليات التي تُنفَّذ في الفضاء الإلكتروني دعما للأعمال العدائية في النزاع المسلح مثلما ينطبق على عمليات عسكرية أخرى.

يسعى القانون الدولي الإنساني إلى الحد من آثار النزاع المسلح – فهو يحمي الأفراد الذين ليسوا مشاركين، أو أنهم لم يعودوا مشاركين، في العمليات القتالية، ويحد من الطرق والسبل التي يلجأ إليها المعتدون في العمليات الحربية. وكما هو مبين أعلاه، اللجوء إلى استخدام القوة في الفضاء الإلكتروني يحكمه قانون دولي غير القانون الدولي الإنساني، وخاصة ميثاق الأمم المتحدة. القانون الدولي الإنساني يسعى إلى الحد من آثار النزاع المسلح، وبالتالي ليس صحيحا أن تطبيقه على العمليات الإلكترونية في النزاع المسلح سوف يشجع عسكرة الفضاء الإلكتروني.

العملية الإلكترونية يمكن أن تعتبر "هجوما" بموجب القانون الدولي الإنساني حين يكون لها آثار مطابقة أو مماثلة لآثار عمل تقليدي يعتبر هجوما. وحين ترقى عملية في الفضاء الإلكتروني إلى أن تعتبر "هجوما"، تنطبق حينها مبادئ التمييز والتناسب والإنسانية والضرورة العسكرية تماما كما تنطبق على هجوم يُنفذ بسبل أخرى. ويلزم على المسؤولين عن التخطيط للهجمات أو اتخاذ قرارات بشأنها أو تنفيذها الوصول إلى قراراتهم على أساس تقييمهم لمعلومات من جميع المصادر تكون متاحة لهم بشكل معقول في الوقت المناسب. ويجب احترام جميع قواعد القانون الدولي الإنساني ذات الصلة لدى التخطيط للعمليات وتنفيذها، سواء كانت عمليات إلكترونية أو بسبل أخرى – حيث إن كون العمليات الإلكترونية معقدة ليس عذرا لتوفير مستوى أقل من الحماية للمدنيين والمنشآت المدنية.

المدنيون محميون من الهجمات ما لم، وإلى حين أن، يشاركوا بشكل مباشر في العمليات العدائية. حين ينفذ مدنيون عمليات إلكترونية في نزاع مسلح ترقى لأن تعتبر هجمات، فإنهم يفقدون الحماية التي يتمتعون بها بموجب القانون الدولي الإنساني. ونظرا لدورهم المباشر في العمليات العدائية، فإنهم يصبحون أهدافا عسكرية مشروعة.

ما يلي مستقبلا

كما أشرنا أعلاه، ترحب المملكة المتحدة بهذه المبادرة كجزء من التعاون المستمر بين الدول لتطوير فهمها لانطباق القانون الدولي على الفضاء الإلكتروني، وتعزيز قدراتها لتحقيق ذلك. وسوف تستمر المملكة المتحدة بكل نشاط في تواصلها مع الدول الأخرى لضمان وضوح كيفية انطباق القانون الدولي على الفضاء الإلكتروني، ومعايير السلوك المسؤول من جانب الدول في الفضاء الإلكتروني. وبفعل ذلك، سيكون من الضروري الانتقال إلى ما هو أبعد من مناقشة المفاهيم والمبادئ

العامة، وتوضيح ما يعتبر سلوكا غير مشروع في القطاعات الأكثر عرضة للتضرر من السلوك الإلكتروني المدمر.

***

导言

1. 国际法对于维护网络空间的安全和稳定至关重要。如同适用于其他行为一样，国际法适用于国家在网络空间的行为。国际社会明确承认国际法适用于国家在网络空间的行为。在最近发布的 2021 年开放成员工作组（OEWG）报告中，各国重申了他们的理解（与 2013 年和 2015 年政府专家组（GGE）报告所述一致），即“国际法，特别是《联合国宪章》对维护国际和平与稳定以及促进一个开放、安全、稳定、无障碍、和平的信通技术环境是适用的和不可或缺的”。

2. 因此，英国欢迎目前的倡议，鼓励各国将声明作为政府专家组报告的附件提交，阐明各国关于国际法如何适用于网络空间的国家立场。这将有助于各国促进对国际法及其发展的更好理解，提高对于什么构成网络空间可接受行为方面的透明度和相互理解。合法行为的界限越清晰，误判的风险就越低，违规的后果也就越清晰。本声明旨在为这一倡议做出贡献，并在非详尽无遗的基础上，简要阐述英国对国际法如何适用于国家在网络空间的行为的若干具体问题的立场。

3. 英国致力于自由、开放、和平和安全的网络空间。网络空间的使用符合各国和整个国际社会的利益，各国有权行使其网络能力，但须遵守国际法规定的任何限制。虽然“网络空间（cyberspace）”没有国际一致同意的定义，但在本声明中，它是指使用相互依存的信息技术基础设施网络开展行动和行为的领域，包括互联网、与互联网相关的电信网络、计算机系统和接入互联网的设备[270]。在本声明中，前缀“cyber（网络）”用于描述使用此类信息技术基础设施进行的活动的特征。

《联合国宪章》

4. 如同适用于其他行为一样，《联合国宪章》适用于国家在网络空间的行为

5. 《联合国宪章》第二条第四项禁止威胁使用武力或使用武力，以任何不符合联合国宗旨的其他方式，侵害任何国家的领土完整或政治独立。如果国家在网络空间实际实施或威胁实施的行为已经具有或可能具有与使用动能手段的行为相同或类似的效果，视每个案件的事实和情况而定，那么该行为有可能构成

[270] 本定义基本建立在英国政府《2016-2021 年国家网络安全战略》对网络空间定义的基础上，具体请参见：https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643429/Chinese_translation_-_National_Cyber_Security_Strategy_2016.pdf。它将网络空间定义为“相互依存的信息技术基础设施网络，包括互联网、电信网络、计算机系统、接入互联网的设备以及嵌入式处理器和控制器。它也可能把虚拟世界或领域称之为一种经验现象或抽象概念。”

威胁使用或使用武力。根据国际法，哪些情况中威胁使用或使用武力不属于违法无关于该种行为是通过动能手段还是网络手段实施的。

6. 如《联合国宪章》第五十一条所确认的那样，通过网络手段实施的行动可能构成武力攻击，从而产生单独或集体自卫的固有权利，在这种情况下，行动的规模和效果等同于使用动能手段进行的武力攻击。考虑攻击规模和效果的因素可能包括（实际或预期）对财产的实体破坏、伤害和死亡。对迫在眉睫或正在进行的武力攻击行使固有的自卫权，无论这种武力攻击是通过动能手段或网络手段实施，对其行使的自卫权本身无论是通过网络或动能手段实施，都必须始终满足必要性和相称性的要求。是否诉诸于行使固有的自卫权始终应认真考虑所有的情况后再决定。

7. 《宪章》第二条第三项和第六章关于和平解决争端的规定同样适用于国家在网络空间的活动。因此，根据第三十三条第一项，如果任何与网络有关的争端的持续可能危及国际和平与安全的维护，该争端的当事国应努力以《宪章》第三十三条所述之和平手段解决争端：谈判、调查、调停、和解、公断、司法解决、诉诸区域机关或区域办法，或当事国自行选择的其他和平方法。

不干涉和主权

8. 在威胁使用或使用武力的门槛之下，禁止干涉国家内政的习惯国际法规则适用于国家在网络空间的行动，如同适用于这些国家的其他活动一样。正如国际法院在尼加拉瓜案的判决中所述，不干涉规则的目的是确保所有国家在会对本国权力产生影响的事务中不受外部强制干预，这些权力是一国主权的核心，如同选择自己的政治、社会、经济和文化制度的自由一样[271]。

9. 正如英国以前注意到的那样，虽然这一规则的确切界限仍然在持续辩论中，但它在国际法中为评估国家行为的合法性提供了明确的基础。因此，利用敌对的网络行动来操纵另一个国家的选举制度以改变选举结果、破坏另一个国家金融系统的稳定、或者针对另一个国家基本医疗服务的行为，根据具体情况，都可能违反国际法禁止干预的规定。

10. 国际法院已经确定，被禁止的干预是根据国家主权原则允许每个国家自由决定的事项。主权作为一项一般原则，是国际法的一个基本概念。英国回顾，

[271] 尼加拉瓜境内和针对尼加拉瓜的军事和准军事活动（尼加拉瓜诉美利坚合众国），案情实质，判决书，《1986 年国际法院案例汇编》，第 205 段：“在这方面，[法院]注意到，鉴于普遍接受的提法，这项原则禁止所有国家或国家集团直接或间接干预他国内政或外交事务。因此，被禁止的干预必须是会对每个国家被允许、且应按照国家主权原则可以自由决定的事项产生影响的干预。其中之一是政治、经济、社会和文化制度的选择，以及外交政策的制定。当使用强制方法干预这种选择时，干预就是错误的，这种选择必须保持自由。无论是以军事行动这种直接形式，还是以支持另一国境内颠覆或恐怖主义武装活动这种间接形式，在使用武力的干预情况中，胁迫因素都尤其明显。而这种胁迫因素，定义了被禁止的干预，也实际上构成了这种干预的本质。”

任何对国家活动的禁止，无论是涉及网络空间还是其他事项，都必须在对有关国家具有约束力的习惯国际法或条约中明确确立。英国认为，主权的一般概念本身并不能提供充分或明确的依据，以推论针对网络行为的一项具体规定或其它禁止超出了上述不干涉原则。与此同时，英国注意到，对这些问题的不同观点不应妨碍各国评估某些特定情况是否构成国际不法行为，并就这些问题得出共同结论。

国家责任和行为归属

11. 根据国际法，一国应对根据国家责任规范可归属于该国的网络活动负责。因此，一国对于在其领土上发生的活动的责任，包括与网络空间活动有关的责任，是根据关于国家责任的国际法规则确定的。例如，根据国际法，一国除了对其机关和代理人的行为承担责任之外，还应对个人或团体按照其指示或在其指挥或控制下做出的行为承担责任。

12. 《联合国打击跨国有组织犯罪公约》规范 13(c)规定，各国不得允许其领土被用于利用信息和通信技术蓄意实施的国际不法行为。这一规范对构成适当的国家行为的要素提供了指导。英国意识到，各国必须在其能力范围内采取适当、合理可用和切实可行的步骤，回应被认为是有害的活动，以便为了所有国家的利益加强网络空间的稳定性。但是，各国将这一规范称为不具约束力的规范，这表明，还没有足够的国家实践来确立适用于网络空间活动的具体的习惯国际法“尽职”规则。

13. “归属”一词在法律和非法律意义上都用于与网络空间相关的情况。从法律意义上来说，它指的是确定国际不法行为的责任人。在非法律意义上，它用于描述识别实施了网络行为的行为体（包括非国家行为体），这些行为可能被视为敌对或恶意行为，但不一定涉及国际不法行为。

14. 对英国而言，在决定是否将此类网络空间活动进行公开归属时，存在技术和外交方面的考虑。是否公开发表归属声明是一个政策问题。每个案件都应根据其本身属性进行考虑。英国将出于促进其对提高网络空间清晰度和稳定性的承诺的原因，或者在符合其自身利益的情况下公开地归属此种活动。

15. 无论归属的性质如何，都没有一般的法律义务要求一国公开披露其作出的行为归属决定所依据的任何基本信息。

反制措施

16. 根据国际法，针对国家在网络空间的活动以及其他活动，可以诉诸反制措施来应对国际不法行为。这包括对其网络活动构成国际不法行为的国家采取反制措施，以及通过网络行动来实施反制措施。反制措施不必是对称的：即，如果国际不法行为本身不是网络活动，回应措施亦可能涉及基于网络的反制措施（反之亦然）。

17. 受害国对国际不法行为的责任国采取反制措施，只能以促使该国遵守其义务为目的。采用的任何措施必须与所受损害相称。实施反制措施必须符合国际法规定的条件和限制，特别是不得违反禁止威胁使用或使用武力的规定，并且必须是促使责任国遵守其义务所必须的、并与其目的相称的，不得违反任何其他国际法强制性规范。

18. 国际法对在网络空间使用反制措施的应用必须考虑到网络活动的性质，这些活动可能几乎在瞬间或短时间内开始，然后停止。在这些情况下，更广泛规模的各种网络活动可能共同构成一种国际不法行为，回应也因此被视为是正当的。

19. 英国不认为采取反制措施的国家在所有情况下都有发出事先通知的法律义务(包括呼吁为国际不法行为负责的国家遵守国际法)。在用反制措施回应隐蔽的网络入侵时，或者在采取本身就依赖于隐蔽网络能力的反制措施时，事先通知可能不是一项法律义务。在这种情况下，事先通知可能暴露敏感性较高的能力，并损害有关反制措施的有效性。但是，在没有事先通知的情况下诉诸反制措施的任何决定必须是必要的，并且与在这种情况下促使遵守法律的目的相称。

国际人权法

20. 人权义务适用于各个国家在网络空间的活动，正如它们适用于其他活动一样。英国继续支持人权理事会第 20/8 号决议中提出的观点，即“人们在线下享有的权利也必须同样在线上得到保护……”。各国有义务按照适用的国际人权法行事，包括习惯国际法，以及他们加入的国际公约，如《公民权利和政治权利国际公约》、其他联合国条约和区域性文书，如《欧洲人权公约》。

21. 各国对网络空间活动中人权义务的尊重对于确保一个开放、安全、稳定、无障碍和和平的环境至关重要，某些权利可能与国家在网络空间的活动特别相关，包括隐私、家庭、住宅或通信不受任意或非法干涉的权利，思想、良心和宗教自由权，以及言论自由权。

《国际人道法》(IHL)

22. 和适用于其他军事行动一样，《国际人道法》也适用于在武装冲突中推动敌对行为的网络空间行动。

23. 《国际人道法》寻求限制武装冲突的影响——它保护没有或不再参与敌对行动的人，并限制交战方使用的战争方法和手段。如上所述，在网络空间诉诸使用武力受《国际人道法》以外的国际法管辖，特别是《联合国宪章》。《国际人道法》寻求限制武装冲突的影响，因此，认为《国际人道法》适用于武装冲突中的网络行动会鼓励网络空间军事化的这种看法是不正确的。

24. 根据《国际人道法》，网络行动有可能成为“攻击”，其效果与构成攻击的动能行动相同或相似。在网络空间的行动构成“攻击”的情况下，区别原则、相

称原则、人道原则和军事必要性原则适用于任何其他方式的攻击。负责策划、决定或实施攻击的人必须根据他们对在相关时间、从所有来源合理获得的信息的评估而做出决定。无论是通过网络还是其他方式，在规划和实施行动时都必须遵守《国际人道法》的所有相关规则——网络行动的复杂性不能成为降低保护平民和民用物体标准的借口。

25. 除非平民参与敌对行动，否则平民是受到保护、免受攻击的。如果平民在武装冲突中实行了构成攻击的网络行动，他们将失去在《国际人道法》中的受保护地位，并通过直接参与敌对行动，成为合法的军事目标。

展望未来

26. 如上所述，作为各国之间正在进行的合作的一部分，英国欢迎这一倡议，以增进各国对国际法在网络空间的适用性的理解，并加强实现这一目标的能力。英国将继续积极与其他国家接触，以确保明确国际法如何适用于网络空间，以及网络空间中负责任的国家行为的界定因素。进行这项工作时，重要的是要超越对一般概念和原则的讨论，要明确哪些行为构成那些最容易受到破坏性网络行为影响的领域的不法行为

***

INTRODUCTION

1. International law is fundamental to maintaining security and stability in cyberspace and international law applies to States' conduct in cyberspace on the same basis as it applies to their other conduct. The application of international law to States' conduct in cyberspace is clearly recognised by the international community. In the recent 2021 OEWG report, States reaffirmed their understanding (as already set out in the 2013 and 2015 GGE reports) that 'international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment'.

2. The United Kingdom therefore welcomes the current initiative encouraging States to submit statements to be annexed to the report of the Governmental Group of Experts setting out their national positions on how international law applies in cyberspace. This will assist States in promoting a better understanding of international law and its development and facilitate greater transparency about, and mutual understanding of, what constitute acceptable behaviours in cyberspace. The greater the clarity on the boundaries of lawful behaviour, the lower the risk of miscalculation and the clearer the consequences can be for transgressing them. This statement is intended as a contribution to this initiative and briefly sets out, on a non-exhaustive basis, the United Kingdom's position on a number of specific issues relating to how international law applies to States' conduct in cyberspace.

3. The United Kingdom is committed to a free, open, peaceful and secure cyberspace. The use of cyberspace is in the interest of States and the international community as a whole and States have the right to exercise their cyber capabilities, subject to any restrictions imposed by international law. While there is no internationally agreed definition of "cyberspace" it is used in this statement to refer to the sphere of actions and conduct carried out using the interdependent network of

information technology infrastructures that includes the internet, internet-related telecommunications networks, computer systems and internet connected devices.[272] The prefix "cyber" is used in this statement to characterise actions which are carried out using such information technology infrastructures.

UN CHARTER

4. The Charter of the United Nations applies to States' conduct in cyberspace, as it does to their other conduct.

5. Article 2(4) of the UN Charter prohibits the threat or use of force against the territorial integrity or political independence of any State or in any other manner inconsistent with the purposes of the United Nations. Depending on the facts and circumstances in each case, conduct by States carried out in cyberspace is capable of constituting a threat or use of force if the actual or threatened conduct has or would have the same or similar effects of conduct using kinetic means. The circumstances in which the threat or use of force is not unlawful under international law are the same irrespective of whether the conduct is by kinetic or cyber means.

6. An operation carried out by cyber means may constitute an armed attack giving rise to the inherent right of individual or collective self-defence, as recognised in Article 51 of the UN Charter where the scale and effects of the operation are equivalent to those of an armed attack using kinetic means. Factors in considering the scale and effects of an attack may include the (actual or anticipated) physical destruction of property, injury and death. The exercise of the inherent right of self-defence against an imminent or on-going armed attack whether by kinetic or cyber means, may itself be by cyber or kinetic means and must always fulfil the requirements of necessity and proportionality. Whether or not to have recourse to the exercise of the inherent right of self-defence will always be carefully considered having regard to all the circumstances.

7. Article 2(3) and the provisions of Chapter VI of the Charter on the peaceful settlement of disputes can equally apply in relation to States' activities in cyberspace. Thus, in accordance with Article 33(1), States that are party to any cyber-related international dispute the continuation of which is likely to endanger the maintenance of international peace and security, shall endeavour to settle such dispute by peaceful means as described in Article 33 of the Charter: negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice.

NON-INTERVENTION & SOVEREIGNTY

8. Below the threshold of the threat or use of force, the customary international law rule prohibiting interventions in the domestic affairs of States applies to States' operations in cyberspace as it does to their other activities. As set out by the International Court of Justice in its judgment in the Nicaragua case, the purpose of

[272] This definition is broadly based on the definition of cyberspace in HMG's National Cyber Security Strategy 2016-2021 which can be found here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf which defines cyberspace as 'the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept.'

the rule on non-intervention is to ensure that all States remain free from external coercive intervention in matters affecting a State's powers, which are at the heart of a State's sovereignty such as the freedom to choose its own political, social, economic and cultural system.[273]

9. As the UK has noted previously, while the precise boundaries of this rule continue to be the subject of on-going debate, it provides a clearly established basis in international law for assessing the legality of State conduct. Thus the use of hostile cyber operations to manipulate the electoral system in another State to alter the results of an election, to undermine the stability of another State's financial system or to target the essential medical services of another State could all, depending on the circumstances, be in violation of the international law prohibition on intervention.

10. The International Court of Justice has established that a prohibited intervention is one bearing on matters which each State is permitted, by the principle of State sovereignty, to decide freely. Sovereignty, as a general principle, is a fundamental concept in international law. The United Kingdom recalls that any prohibition on the activities of States whether in relation to cyberspace or other matters, must be clearly established either in customary international law or in a treaty binding upon the States concerned. The United Kingdom does not consider that the general concept of sovereignty by itself provides a sufficient or clear basis for extrapolating a specific rule or additional prohibition for cyber conduct going beyond that of non-intervention referred to above. At the same time, the United Kingdom notes that differing viewpoints on such issues should not prevent States from assessing whether particular situations amount to internationally wrongful acts and arriving at common conclusions on such matters.

STATE RESPONSIBILITY & ATTRIBUTION

11. A State is responsible under international law for cyber activities that are attributable to it in accordance with the rules on State responsibility. The responsibility of a State for activities that occur on its territory including in relation to activities in cyberspace is therefore determined in accordance with the rules of international law on State responsibility. As well as bearing responsibility for acts of its organs and agents, a State is also responsible in accordance with international law where, for example, a person or a group of persons acts on its instructions or under its direction or control.

12. UNGGE Norm 13(c) provides that States should not knowingly allow their territory to be used for internationally wrongful acts using information and communications technology. This norm provides guidance on what may be expected to constitute appropriate State behaviour. The UK recognises the importance of

[273] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America),* Merits, Judgment, ICJ Reports 1986 at para 205: 'In this respect [the Court] notes that, in view of the generally accepted formulations, the principle forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.'

States taking appropriate, reasonably available, and practicable steps within their capacities to address activities that are acknowledged to be harmful in order to enhance the stability of cyberspace in the interest of all States. But the fact that States have referred to this as a non-binding norm indicates that there is not yet State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace.

13. The term 'attribution' is used in relation to cyberspace in both a legal and non-legal sense. It is used in a legal sense to refer to identifying those who are responsible for an internationally wrongful act. It is also used in a non-legal sense to describe the identification of actors (including non-state actors) who have carried out cyber conduct which may be regarded as hostile or malicious but does not necessarily involve an internationally wrongful act.

14. For the UK, there are technical and diplomatic considerations in determining whether to attribute publicly such activities in cyberspace. The decision whether to make a public attribution statement is a matter of policy. Each case is considered on its merits. The UK will publicly attribute conduct in furtherance of its commitment to clarity and stability in cyberspace or where it is otherwise in its interests to do so.

15. Whatever the nature of the attribution, there is no general legal obligation requiring a State to publicly disclose any underlying information on which its decision to attribute conduct is based.

COUNTERMEASURES

16. Resort may be had to countermeasures in response to an internationally wrongful act, in accordance with international law, in relation to States' activities in cyberspace as in relation to their other activities. This includes both resorting to countermeasures against a State whose cyber activities constitute internationally wrongful acts and carrying out countermeasures by means of cyber operations. Countermeasures need not be symmetrical: where the internationally wrongful act is itself not a cyber activity, the response may nonetheless involve cyber-based countermeasures (and vice versa).

17. An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations. Any measures adopted must be commensurate with the injury suffered. They must be carried out in accordance with the conditions and restrictions established in international law and must in particular not contravene the prohibition on the threat or use of force, must be necessary and proportionate to the purpose of inducing the responsible State to comply with its obligations and must not contravene any other peremptory norm of international law.

18. The application of international law to the use of countermeasures in cyberspace must take account of the nature of cyber activities, which might commence and then cease almost instantaneously or within a short timeframe. In those circumstances, a wider pattern of cyber activities might collectively constitute an internationally wrongful act justifying a response.

19. The UK does not consider that States taking countermeasures are legally obliged to give prior notice (including by calling on the State responsible for the internationally wrongful act to comply with international law) in all circumstances. Prior notice may not be a legal obligation when responding to covert cyber intrusion with countermeasures or when resort is had to countermeasures which themselves depend on covert cyber capabilities. In such cases, prior notice could expose highly sensitive capabilities and prejudice the very effectiveness of the countermeasures in

question. However any decision to resort to countermeasures without prior notice must be necessary and proportionate to the purpose of inducing compliance in the circumstances.

INTERNATIONAL HUMAN RIGHTS LAW

20. Human rights obligations apply to States' activities in cyberspace as they do to in relation to their other activities. The UK continues to support the view set out in Human Rights Council Resolution 20/8 that 'the same rights that people have offline must also be protected online…'. States have an obligation to act in accordance with applicable international human rights law, including customary international law, and international conventions to which they are a party, such as the International Covenant on Civil and Political Rights, other UN treaties, and regional instruments such as the European Convention on Human Rights.

21. States' respect for their human rights obligations in relation to their activities in cyberspace is essential to ensuring an open, secure, stable, accessible and peaceful environment and certain rights may have particular relevance to States' activities in cyberspace including the right not to be subjected to arbitrary or unlawful interference with privacy, family, home or correspondence, the right to freedom of thought, conscience and religion and the right to freedom of expression.

INTERNATIONAL HUMANITARIAN LAW (IHL)

22. IHL applies to operations in cyberspace conducted in the furtherance of hostilities in armed conflict just as it does to other military operations.

23. IHL seeks to limit the effects of armed conflict - it protects persons who are not, or who are no longer, participating in hostilities, and limits the methods and means of warfare employed by the belligerents. As noted above, recourse to the use of force in cyberspace is governed by international law other than IHL, in particular the UN Charter. IHL seeks to limit the effects of armed conflict and it is not therefore correct that its applicability to cyber operations in armed conflict would encourage the militarisation of cyberspace.

24. A cyber operation is capable of being an 'attack' under IHL where it has the same or similar effects to kinetic action that would constitute an attack. Where an operation in cyberspace amounts to an 'attack', the principles of distinction, proportionality, humanity and military necessity apply in the same way as they do to an attack by any other means. Those responsible for planning, deciding upon, or executing attacks necessarily have to reach decisions on the basis of their assessment of the information from all sources which is reasonably available to them at the relevant time. All relevant rules of IHL must be observed when planning and conducting operations whether by cyber or other means – the complexity of cyber operations is no excuse for a lower standard of protection to be afforded to civilians and civilian objects.

25. Civilians are protected from attack unless and for such time as they take a direct part in hostilities. To the extent that civilians carry out cyber operations in an armed conflict that amount to attacks, they would lose their protected status under IHL and, by taking a direct part in hostilities, become legitimate military targets.

LOOKING FORWARD

26. As noted above, the United Kingdom welcomes this initiative as part of ongoing cooperation between States to develop their understanding of the application of international law to cyberspace and the reinforcement of their capacities to achieve this.

The UK will continue actively to engage with other States to ensure that how international law applies to cyberspace and the parameters of responsible State behaviour in cyberspace are clear. In so doing, it will be important to move beyond discussion of general concepts and principles, and to be clear about what constitutes unlawful conduct in those sectors which are most vulnerable to destructive cyber conduct.

***

INTRODUCTION

1. Le droit international est fondamental au maintien de la sécurité et de la stabilité dans le cyberespace, et ce droit international s'applique à la conduite des États dans le cyberespace au même titre qu'il s'applique à leurs autres conduites. L'application du droit international à la conduite des États dans le cyberespace est reconnue clairement par la communauté internationale. Dans le rapport récent (2021) du Groupe de travail à composition non limitée, les États ont réaffirmé leur compréhension (auparavant énoncée dans les rapports 2013 et 2015 du Groupe d'experts gouvernementaux) selon laquelle « le droit international, et en particulier la Charte des Nations Unies, est applicable et est essentiel pour maintenir la paix et la stabilité et promouvoir un environnement informatique ouvert, sûr, stable, accessible et pacifique ».

2. Le Royaume-Uni se réjouit donc de l'actuelle initiative qui encourage les États à soumettre des déclarations, qui seront annexées au rapport du Groupe d'experts gouvernementaux, pour expliquer leur position nationale sur la façon dont le droit international s'applique dans le cyberespace. Elles aideront les États à promouvoir une meilleure compréhension du droit international et de son développement et encourageront une plus grande transparence quant à ce qui constitue des comportements acceptables dans le cyberespace et une compréhension mutuelle en la matière. Plus il y a de clarté sur les limites d'un comportement licite, plus le risque d'erreur d'appréciation est faible et plus les conséquences de leur franchissement peuvent être claires. La présente déclaration a pour objet de contribuer à cette initiative. Elle explique brièvement, de manière non exhaustive, la position du Royaume-Uni sur plusieurs questions précises liées à la façon dont le droit international s'applique à la conduite des États dans le cyberespace.

3. Le Royaume-Uni est résolument en faveur d'un cyberespace libre, ouvert, pacifique et sûr. L'utilisation du cyberespace est dans l'intérêt des États et de l'ensemble de la communauté internationale, et les États ont le droit d'exercer leurs cybercapacités, sauf restrictions imposées par le droit international. S'il n'existe pas de définition internationalement acceptée du cyberespace, le terme désigne dans la présente déclaration le domaine des actions et des conduites menées à l'aide du réseau interdépendant des infrastructures des technologies de l'information qui comprend l'Internet, les réseaux de télécommunications liés à l'Internet, les systèmes informatiques et les appareils connectés à l'Internet[274]. Le préfixe

[274] Cette définition se fonde plus ou moins sur celle du cyberespace donnée dans la Stratégie nationale de cybersécurité 2016-2021 du gouvernement britannique, accessible ici : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_

« cyber » est utilisé dans la présente déclaration pour caractériser des actions qui sont effectuées à l'aide de telles infrastructures des technologies de l'information.

CHARTE DES NATIONS UNIES

4. La Charte des Nations Unies s'applique à la conduite des États dans le cyberespace comme elle s'applique à leurs autres conduites.

5. L'article 2(4) de la Charte de l'ONU interdit le recours à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies. En fonction des faits et des circonstances dans chaque cas, la conduite des États dans le cyberespace peut constituer une menace ou un emploi de la force si cette conduite réelle ou menace de conduite a ou pourrait avoir les mêmes effets ou des effets similaires à ceux d'une conduite faisant usage de moyens cinétiques. Les circonstances dans lesquelles la menace ou l'emploi de la force n'est pas illicite en vertu du droit international sont les mêmes, que la conduite soit menée par des moyens cinétiques ou des cybermoyens.

6. Une opération menée par des cybermoyens peut constituer une agression armée donnant lieu au droit naturel de légitime défense, individuelle ou collective, reconnu par l'article 51 de la Charte de l'ONU lorsque l'échelle et les effets de l'opération sont équivalents à ceux d'une agression armée ayant recours à des moyens cinétiques. Les facteurs dont il y a lieu de tenir compte pour déterminer l'échelle et les effets d'une agression pourront inclure la destruction physique de biens, les préjudices et les pertes de vie humaine (réels ou anticipés). L'exercice du droit naturel de légitime défense contre une agression armée imminente ou en cours, soit par moyens cinétiques, soit par cybermoyens, peut lui-même se faire par des moyens cinétiques ou des cybermoyens et doit toujours satisfaire aux exigences de nécessité et de proportionnalité. La décision d'avoir ou non recours à l'exercice du droit naturel de légitime défense sera toujours examinée attentivement eu égard à toutes les circonstances.

7. L'article 2(3) et les dispositions du chapitre VI de la Charte relatifs au règlement pacifique des différends peuvent s'appliquer également aux activités des États dans le cyberespace. Ainsi, conformément à l'article 33(1), les États parties à tout différend international lié à une question cyber dont la prolongation est susceptible de menacer le maintien de la paix et de la sécurité internationales doivent tenter d'en rechercher la solution par des moyens pacifiques tels qu'ils sont décrits dans l'article 33 de la Charte : négociation, enquête, médiation, conciliation, arbitrage, règlement judiciaire, recours aux organismes ou accords régionaux, ou tout autre moyen pacifique de leur choix.

NON-INTERVENTION ET SOUVERAINETÉ

8. En dessous du seuil de la menace ou de l'emploi de la force, la règle du droit international coutumier interdisant les interventions dans les affaires intérieures des États s'applique aux opérations des États dans le cyberespace comme elle s'applique

data/file/643419/French_translation_-_National_Cyber_Security_Strategy_2016.pdf. Elle définit le cyberespace comme étant « le réseau interdépendant d'infrastructures technologiques informatiques comprenant l'Internet, les réseaux de télécommunications, systèmes informatiques, appareils interconnectés, processeurs et contrôleurs intégrés. Le cyberespace peut également désigner le monde ou domaine virtuel en tant que phénomène vécu ou concept abstrait ».

à leurs autres activités. Comme le stipule la Cour internationale de justice dans son arrêt dans l'affaire du Nicaragua, le but de la règle de non-intervention est de veiller à ce que tous les États demeurent à l'abri de toute intervention coercitive externe dans des matières affectant leurs pouvoirs, qui sont au cœur de la souveraineté de tout État, telle que la liberté de choisir son propre système politique, social, économique et culturel[275].

9. Comme l'a relevé le Royaume-Uni auparavant, si les limites précises de cette règle continuent de faire l'objet d'un débat actuel, elle fournit une base clairement établie dans le droit international pour évaluer la légalité de la conduite d'un État. Ainsi, des cyberopérations hostiles lancées pour manipuler le système électoral d'un autre État en vue de falsifier les résultats d'une élection, mettre à mal la stabilité du système financier d'un autre État ou cibler les services médicaux essentiels d'un autre État pourraient toutes, selon les circonstances, être en violation de l'interdiction d'intervention en vertu du droit international.

10. La Cour internationale de justice a disposé qu'une intervention interdite est une intervention portant sur des matières à propos desquelles chaque État peut, en vertu du principe de souveraineté des États, se décider librement. La souveraineté, en tant que principe général, est un concept fondamental en droit international. Le Royaume-Uni rappelle que toute interdiction des activités des États, que ce soit en lien avec le cyberespace ou d'autres matières, doit être clairement prévue soit dans le droit international coutumier, soit dans un traité contraignant pour les États concernés. Le Royaume-Uni ne considère pas que le concept général de souveraineté offre en lui-même une base suffisante ou claire pour déduire par extrapolation une règle spécifique ou une interdiction supplémentaire pour toute conduite dans le cyberespace au-delà de celle de la non-intervention mentionnée plus haut. En même temps, le Royaume-Uni note que les points de vue divergents sur de telles questions ne devraient pas empêcher les États d'évaluer si certaines situations constituent des faits internationalement illicites et de parvenir à des conclusions communes sur ces questions.

RESPONSABILITÉ DES ÉTATS ET ATTRIBUTION

11. Tout État est responsable en vertu du droit international des cyberactivités qui lui sont attribuables conformément aux règles sur la responsabilité des États. La responsabilité de tout État en ce qui concerne des activités qui ont lieu sur son territoire, y compris des activités liées au cyberespace, est donc déterminée conformément aux règles du droit international sur la responsabilité des États. Outre qu'il assume la responsabilité des actes de ses organes et agents, tout État est également responsable en vertu du droit international lorsque, par exemple, une

[275] *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua* c. *États-Unis d'Amérique),* Fond, Arrêt, Recueil d'arrêts CIJ 1986 au par. 205 : « À cet égard, [la Cour] note que, d'après les formulations généralement acceptées, ce principe interdit à tout État ou groupe d'États d'intervenir directement ou indirectement dans les affaires intérieures ou extérieures d'un autre État. L'intervention interdite doit donc porter sur des matières à propos desquelles le principe de souveraineté des États permet à chacun d'entre eux de se décider librement. Il en est ainsi du choix du système politique, économique, social et culturel et de la formulation des relations extérieures. L'intervention est illicite lorsqu'à propos de ces choix, qui doivent demeurer libres, elle utilise des moyens de contrainte. Cet élément de contrainte, constitutif de l'intervention prohibée et formant son essence même, est particulièrement évident dans le cas d'une intervention utilisant la force, soit sous la forme directe d'une action militaire soit sous celle, indirecte, du soutien à des activités armées subversives ou terroristes à l'intérieur d'un autre État. »

personne ou un groupe de personnes agit sur ses instructions ou sous sa direction ou son contrôle.

12. La norme 13(c) du Groupe d'experts gouvernementaux des Nations Unies prévoit que les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications. Cette norme donne des indications sur ce qui peut être considéré comme constituant un comportement approprié des États. Le Royaume-Uni reconnaît qu'il est important que les États prennent des mesures appropriées, raisonnablement disponibles et possibles dans les limites de leurs capacités pour parer aux activités qui sont reconnues préjudiciables afin de renforcer la stabilité du cyberespace dans l'intérêt de tous les États. Or, le fait que les États ont qualifié ce texte de norme non contraignante indique qu'il n'existe pas encore de pratique étatique suffisante pour inscrire dans le droit international coutumier une règle précise de « diligence raisonnable » applicable aux activités dans le cyberespace.

13. Le terme « attribution » est employé dans le cadre du cyberespace à la fois au sens juridique et non juridique. Il est utilisé dans un sens juridique pour désigner l'identification des responsables d'un fait internationalement illicite. Il est également utilisé dans un sens non juridique pour décrire l'identification d'acteurs (y compris d'acteurs non étatiques) qui ont mené des actions dans le cyberespace pouvant être considérées comme hostiles ou malveillantes mais n'impliquant pas forcément un fait internationalement illicite.

14. Pour le Royaume-Uni, certains aspects techniques et diplomatiques doivent être pris en compte pour déterminer s'il faut attribuer publiquement de telles activités dans le cyberespace. La décision de faire une déclaration publique d'attribution est une question de politique. Chaque décision est prise au cas par cas. Le Royaume-Uni attribuera publiquement une conduite aux fins de son engagement en faveur de la clarté et de la stabilité dans le cyberespace ou lorsque cela est de toute autre manière dans ses intérêts de le faire.

15. Quelle que soit la nature de l'attribution, il n'existe pas d'obligation juridique générale exigeant d'un État qu'il rende publiques les éventuelles informations de base sur lesquelles repose sa décision d'attribuer une conduite.

CONTRE-MESURES

16. Un recours à des contre-mesures est possible en réponse à un fait internationalement illicite, conformément au droit international, dans le cadre des activités des États dans le cyberespace comme dans le cadre d'autres activités. Il peut s'agir à la fois de recourir à des contre-mesures contre un État dont les cyberactivités constituent des faits internationalement illicites et de prendre des contre-mesures au moyen de cyberopérations. Les contre-mesures n'ont pas besoin d'être symétriques : si le fait internationalement illicite n'est pas lui-même une cyberactivité, la réponse peut toutefois impliquer des contre-mesures dans le cyberespace (et vice-versa).

17. Tout État lésé ne peut prendre des contre-mesures contre un État responsable d'un fait internationalement illicite que pour persuader cet État à respecter ses obligations. Toute mesure adoptée doit être proportionnée au préjudice subi. Elle doit être mise en œuvre conformément aux conditions et aux restrictions prévues par le droit international et ne doit pas notamment contrevenir à l'interdiction de menace ou d'emploi de la force, elle doit être nécessaire et en rapport avec le but de

persuader l'État responsable à respecter ses obligations, et ne doit enfreindre aucune autre norme impérative du droit international.

18. L'application du droit international à l'emploi de contre-mesures dans le cyberespace doit tenir compte de la nature des cyberactivités, lesquelles pourraient commencer puis cesser presque instantanément ou dans un bref délai. Dans ces circonstances, un schéma plus large de cyberactivités pourrait collectivement constituer un fait internationalement illicite justifiant une réponse.

19. Le Royaume-Uni ne considère pas que les États qui prennent des contre-mesures soient légalement tenus d'en donner un préavis (notamment en appelant l'État responsable du fait internationalement illicite à se conformer au droit international) en toutes circonstances. Il se peut en effet qu'un préavis ne soit pas une obligation légale lorsqu'un État répond à une cyberintrusion secrète par des contre-mesures ou lorsqu'il recourt à des contre-mesures qui elles-mêmes dépendent de cybercapacités secrètes. En pareils cas, tout préavis risque d'exposer des capacités hautement sensibles et de porter atteinte à l'efficacité même des contre-mesures en question. Toutefois, toute décision de recourir à des contre-mesures sans préavis doit être nécessaire et proportionnée au but d'induire la conformité dans les circonstances.

DROIT INTERNATIONAL DES DROITS DE L'HOMME

20. Les obligations relevant des droits de l'homme s'appliquent aux activités des États dans le cyberespace comme elles s'appliquent à leurs autres activités. Le Royaume-Uni continue de soutenir le point de vue exposé dans la résolution 20/8 du Conseil des droits de l'homme selon laquelle « les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne ». Les États sont tenus d'agir conformément à la législation internationale applicable relative aux droits de l'homme, y compris au droit international coutumier et aux conventions internationales auxquelles ils sont parties, tels le Pacte international relatif aux droits civils et politiques, les autres traités de l'ONU et les instruments régionaux tels que la Convention européenne des droits de l'homme.

21. Il est essentiel que les États respectent leurs obligations en matière de droits de l'homme dans le cadre de leurs activités dans le cyberespace afin de garantir un environnement ouvert, sûr, stable, accessible et pacifique. En outre, certains droits peuvent revêtir une importance particulière pour les activités des États dans le cyberespace, notamment le droit de ne pas subir d'ingérence arbitraire ou illicite dans la vie privée, la famille, le foyer ou la correspondance, le droit à la liberté de pensée, de conscience et de religion, et le droit à la liberté d'expression.

DROIT INTERNATIONAL HUMANITAIRE (DIH)

22. Le droit international humanitaire (DIH) s'applique aux opérations menées dans le cyberespace au service d'hostilités dans les conflits armés tout comme il s'applique à d'autres opérations militaires.

23. Le DIH cherche à limiter les effets des conflits armés. Il protège ceux et celles qui ne participent pas ou plus aux hostilités, et limite les méthodes et les moyens de combat auxquels les belligérants peuvent recourir. Comme indiqué ci-dessus, le recours à l'emploi de la force dans le cyberespace est régi par une législation internationale autre que le DIH, en particulier par la Charte des Nations Unies. Le DIH cherche à limiter les effets des conflits armés et il n'est donc pas correct que

son applicabilité aux cyberopérations menées dans les conflits armés encourage la militarisation du cyberespace.

24. Une cyberopération peut constituer une « agression » au titre du DIH lorsqu'elle a les mêmes effets ou des effets similaires à une action cinétique qui constituerait une agression. Lorsqu'une opération menée dans le cyberespace équivaut à une « agression », les principes de distinction, de proportionnalité, d'humanité et de nécessité militaire s'appliquent de la même manière qu'ils s'appliquent à une agression lancée par tout autre moyen. Les personnes responsables de planifier, de décider ou d'exécuter des attaques doivent nécessairement fonder leurs décisions sur leur évaluation des renseignements émanant de toutes les sources qui leur sont raisonnablement disponibles au moment voulu. Toutes les règles applicables du DIH doivent être observées lors de la planification et de la conduite d'opérations, qu'elles soient menées par des cybermoyens ou par d'autres moyens – la complexité des cyberopérations n'est pas un prétexte pour accorder aux civils et aux biens civils un niveau de protection plus faible.

25. Les civils sont protégés contre les agressions, à moins qu'ils ne participent directement aux hostilités et pendant la durée de cette participation. Dans la mesure où des civils mèneraient dans un conflit armé des cyberopérations qui équivalent à des agressions, ils perdraient le statut de protection que leur confère le DIH et, en prenant directement part aux hostilités, deviendraient des cibles militaires légitimes.

À L'AVENIR

26. Comme indiqué ci-dessus, le Royaume-Uni accueille favorablement cette initiative dans le cadre d'une coopération permanente entre les États pour développer leur compréhension de l'application du droit international au cyberespace et renforcer leurs capacités pour y parvenir. Le Royaume-Uni poursuivra sa coopération active avec les autres États pour faire en sorte que la façon dont le droit international s'applique au cyberespace et les paramètres définissant le comportement responsable des États dans le cyberespace soient clairs. Ce faisant, il sera important de dépasser les concepts et les principes généraux et d'établir clairement en quoi consiste une conduite illicite dans les secteurs qui sont les plus exposés à des cyberactivités destructives.

***

ВВЕДЕНИЕ

1. Международное право имеет основополагающее значение для поддержания безопасности и стабильности в киберпространстве, и нормы международного права применимы к поведению государств в киберпространстве, так же, как они применимы к их поведению в других сферах. Применимость норм международного права к поведению государств в киберпространстве со всей очевидностью признается международным сообществом. В недавнем докладе РГОС за 2021 год государства вновь подтвердили понимание того (как уже указывалось в докладах ГПЭ за 2013 и 2015 гг.), что нормы международного права, и в частности Устав Организации Объединенных Наций, применимы и имеют существенно важное значение для поддержания мира и стабильности и создания открытой, безопасной, мирной и доступной ИКТ-среды.

2. Поэтому Соединенное Королевство Великобритании и Северной Ирландии приветствует текущую инициативу, поощряющую государства

представить для включения в приложение к докладу Группы правительственных экспертов заявления с изложением их национальных позиций о применимости норм международного права в киберпространстве. Это будет содействовать лучшему пониманию норм международного права и их разработки, а также большей транспарентности и взаимопониманию в отношении того, что представляет собой допустимое поведение в киберпространстве. Чем четче будут определены границы правового поведения, тем меньше опасность совершения ошибки и тем четче понимание последствий нарушения этих границ. В настоящем заявлении, представленном в рамках этой инициативы, кратко, на неисчерпывающей основе, изложена позиция Соединенного Королевства Великобритании и Северной Ирландии по ряду конкретных вопросов, касающихся применимости норм международного права к поведению государств в киберпространстве.

3. Соединенное Королевство Великобритании и Северной Ирландии привержено делу сохранения свободного, открытого и безопасного киберпространства. Использование киберпространства отвечает интересам государств и международного сообщества в целом, и государства вправе использовать свои кибервозможности при условии соблюдения ограничений, налагаемых международным правом. Хотя определение «киберпространства» не согласовано на международном уровне, в настоящем заявлении оно используется в отношении сферы действий и поведения, осуществляемых с использованием взаимосвязанной и взаимозависимой сети информационных технологических инфраструктур, включая интернет, связанные с интернетом телекоммуникационные сети, компьютерные системы и подключенные к интернету устройства[276]. Префикс «кибер» используется в настоящем заявлении для описания действий, которые выполняются с использованием таких информационных технологических инфраструктур.

УСТАВ ООН

4. Устав Организации Объединенных Наций применим к поведению государств в киберпространстве так же, как и к поведению в других областях.

5. Статья 2(4) Устава ООН запрещает угрозу силой или ее применение против территориальной неприкосновенности или политической независимости любого государства или каким-либо другим образом, несовместимым с целями Объединенных Наций. В зависимости от фактов и обстоятельств в каждом конкретном случае поведение государства в киберпространстве может представлять собой угрозу силой или ее применение, если фактическое действие или угроза его применения имеет или могло бы иметь такой же или подобный эффект, как поведение с использованием кинетических средств. Определения обстоятельств, при которых угроза силой или ее применение не расцениваются как

[276] Данное определение в целом основывается на определении кибепространства, данном в «Национальной стратегии кибербезопасности 2016–2021» правительства Великобритании, доступное по ссылке: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/ttachment_data/file/643426/Russian_translation_-_National_Cyber_Security_Strategy_2016.pdf, которое определяет киберпространство как «взаимосвязанную и взаимозависимую сеть информационных технологических инфраструктур, включая интернет, телекоммуникационные сети, компьютерные системы, взаимосвязанные устройства и встроенные процессы и контролеры. Этот термин также может относиться к виртуальном миру или среде, где он обозначает феномен, переживаемый людьми, или абстрактную концепцию».

противоправные согласно международному праву, являются одними и теми же вне зависимости от того, совершается ли поведение с использованием кинетических или кибернетических средств.

6. Операция, осуществляемая с применением киберсредств, может представлять собой вооруженное нападение, обусловливающее осуществление неотъемлемого права на индивидуальную или коллективную самооборону в соответствии со Статьей 51 Устава ООН, если по своим масштабам и последствиям эта операция сопоставима с вооруженным нападением с применением кинетических средств. Факторы, которые необходимо учитывать при оценке масштабов и последствий нападения, могут включать в себя (фактическое или ожидаемое) физическое разрушение имущества, увечье или гибель людей. Неотъемлемое право на самооборону в случае неизбежного или фактического вооруженного нападения, будь то с применением кинетических или кибернетических средств, также может осуществляться с применением кибернетических или кинетических средств и должно всегда удовлетворять требованиям необходимости и пропорциональности. Решение об осуществлении неотъемлемого права на самооборону следует всегда тщательно взвешивать с учетом всех обстоятельств.

7. Статья 2(3) и положения Главы VI Устава о мирном разрешении споров могут быть также применимы к действиям государств в киберпространстве. Таким образом, согласно Статье 33(1) государства, участвующие в любом международном споре, связанном с киберпространством, продолжение которого могло бы угрожать поддержанию международного мира и безопасности, должны стараться разрешить такой спор при помощи мирных средств, как описано в Статье 33 Устава: путем переговоров, обследования, посредничества, примирения, арбитража, судебного разбирательства, обращения к региональным органам или соглашениям или иными мирными средствами по своему выбору.

НЕВМЕШАТЕЛЬСТВО И СУВЕРЕНИТЕТ

8. Нормы международного обычного права, запрещающие вмешательство во внутренние дела государств, применимы к операциям государств, осуществляемым в киберпространстве на уровне ниже угрозы силой или ее применения, так же как они применимы к другим видам их деятельности. Как указывает Международный Суд в своем решении по делу Никарагуа, основное содержание принципа невмешательства заключается в обеспечении свободы всех государств от внешнего вмешательства с использованием методов принуждения в дела, затрагивающие властные полномочия государства, которые лежат в основе принципа государственного суверенитета, например, свободы принимать решения, такие как выбор политической, социальной, экономической и культурной систем[277].

[277] *Дело о военной и военизированной деятельности в Никарагуа и против Никарагуа (Никарагуа против Соединенных Штатов Америки),* Решение по существу дела, Отчеты МС 1986, пункт 205: «В этом отношении [Суд] отмечает, что ввиду общепринятых формулировок данный принцип запрещает всем государствам или группам государств вмешиваться, прямо или косвенно, во внутренние или внешние дела других государств. Соответственно, запрещенным вмешательством должно быть вмешательство, имеющее отношение к вопросам, по которым каждое государство — в соответствии с принципом государственного суверенитета — может свободно принимать решения. Одним из них является выбор политической, экономической, социальной и культурной системы и выработка внешней политики. Вмешательство

9. Хотя, как отмечалось Великобританией ранее, точные границы этого принципа по-прежнему остаются предметом продолжающейся дискуссии, он обеспечивает четкую основу в рамках международного права для вынесения оценки о правомерности поведения государства. Таким образом, проведение враждебных кибероперации в целях манипулирования избирательной системой другого государства, направленное на изменение результатов выборов, на подрыв стабильности финансовой системы другого государства или против важных медицинских служб другого государства может, в зависимости от обстоятельств, быть расценено как нарушение норм международного права, запрещающих вмешательство.

10. Международный Суд установил, что запрещенным вмешательством должно быть вмешательство, имеющее отношение к вопросам, по которым каждое государство — в соответствии с принципом государственного суверенитета — может свободно принимать решения. Суверенитет, как общий принцип, является одной из фундаментальных концепций международного права. Соединенное Королевство Великобритании и Северной Ирландии напоминает, что любое запрещение деятельности государств, будь то в отношении кибепространства или других вопросов, должно быть четко определено либо в обычном международном праве, либо в договоре, имеющим обязательную силу для причастных государств. Соединенное Королевство Великобритании и Северной Ирландии не считает, что общий принцип суверенитета сам по себе обеспечивает достаточную или четкую основу для экстраполяции той или иной нормы или дополнительного запрещения поведения в киберпространстве, которое выходит за рамки невмешательства, упомянутого выше. Вместе с тем Соединенное Королевство Великобритании и Северной Ирландии отмечает, что наличие разных точек зрения по этим вопросам не должно помешать государствам выносить оценку о том, составляет ли та или иная ситуация международно-противоправное деяние, и приходить к общим выводам по этим вопросам.

ОТВЕТСТВЕННОСТЬ ГОСУДАРСТВ И ПРИСВОЕНИЕ ОТВЕТСТВЕННОСТИ

11. Согласно международному праву, государство несет ответственность за кибердействия, приписываемые ему в соответствии с положениями об ответственности государств. Таким образом, ответственность государства за действия, совершаемые на его территории, в том числе за действия в киберпространстве, подлежит определению в соответствии с нормами международного права об ответственности государств. Согласно нормам международного права государство несет ответственность не только за действия своих органов и агентов, но и, например, за действия отдельных лиц или групп лиц, которые осуществляются по его указанию либо под его руководством или контролем.

12. Норма 13(c) ГПЭООН предусматривает, что государства не должны заведомо позволять использовать их территорию для совершения международно-противоправных деяний с использованием информационных и

неправомерно, если в связи с осуществлением такого выбора, который должен быть свободным, применяются методы принуждения. Элемент принуждения, который определяет и, более того, формирует содержание принципа, запрещающего вмешательство, особенно очевиден в случае вмешательства с применением силы, либо в прямой форме военных действий, либо в косвенной форме поддержки подрывной или террористической деятельности в другом государстве».

коммуникационных технологий. Данная норма содержит рекомендации о том, что может составлять надлежащее поведение государства. Великобритания признает важность принятия государствами надлежащих, практически доступных и практически реализуемых мер в рамках их возможностей в целях реагирования на действия, признанные вредоносными, чтобы укрепить стабильность в киберпространстве в интересах всех государств. Однако тот факт, что государства называют эту норму необязательной, указывает на отсутствие государственной практики, достаточной для установления конкретной нормы международного права «due diligence», применимой к действиям в киберпространстве.

13. Термин «присвоение ответственности» применяется в отношении киберпространства как в юридическом, так и неюридическом смысле. В юридическом смысле он применяется для определения лиц, ответственных за совершение международно-противоправного деяния. В неюридическом смысле он применяется для описания определения субъектов (включая негосударственных субъектов), которые совершили в киберпространстве поведение, которое может расцениваться как враждебное или злонамеренное, однако не обязательно связано с совершением международно-противоправного деяния.

14. Великобритания считает, что существуют факторы технического и дипломатического характера, которые следует учитывать в решениях о публичном присвоении ответственности за подобные действий в киберпространстве. Решение о выступлении с публичным заявлением о присвоении ответственности, является политическим. Каждый случай следует рассматривать по существу. Великобритания будет публично присваивать ответственность во исполнение своих обязательство по обеспечению ясности и стабильности в киберпространстве или в случаях, когда это в ее интересах по иным причинам.

15. Какой бы ни была природа присвоения ответственности, не существует общего правового обязательства, требующего от государств публично раскрывать любую информацию, на которой основывается решение о присвоении ответственности за поведение.

КОНТРМЕРЫ

16. В соответствии с международным правом контрмеры в ответ на совершение международно-противоправного деяния можно применять в отношении деятельности государств в киберпространстве, так же как и отношении деятельности в других сферах. Сюда входит как применение контрмер против государства, действия которого в киберпространстве представляют собой международно-противоправные деяния, так и применение контрмер путем проведения кибероперациий. Контрмеры не должны быть симметричными: в случаях, если международно-противоправное деяние само по себе не является кибердействием, ответ, тем не менее, может быть связан с применением контрмер в киберпространстве (и наоборот).

17. Любое пострадавшее государство вправе применять контрмеры против государства, ответственного за совершение международно-противоправного деяния, только чтобы принудить это государство к выполнению своих обязательств. Любые принятые контрмеры должны быть соразмерны понесенному ущербу. Контрмеры следует осуществлять в соответствии с условиями и ограничениями, предусмотренными международным правом. В частности, они не должны нарушать запрет на угрозу силой или ее

применение, должны быть необходимы и пропорциональны целям принуждения несущего ответственность государства к исполнению его обязательств и не должны противоречить никакой иной императивной норме международного права.

18. Применение международного права к использованию контрмер в киберпространстве должно учитывать характер кибердействий, которые могут начаться и затем прекратиться практически мгновенно или по истечении короткого времени. В таких обстоятельствах более широкие модели кибердействий могут в совокупности представлять собой международно-противоправное деяние, оправдывающее реагирование.

19. Великобритания не считает, что государства, принимающие контрмеры, несут правовое обязательство по предварительному уведомлению (в том числе путем обращения к государству, ответственному за совершение международно-противоправного деяния, с требованием о соблюдении им международного права) во всех обстоятельствах. Государства могут не иметь правового обязательства по предварительному уведомлению в случае реагирования на тайное кибервторжение с применением контрмер или в случае, если само применение контрмер зависит от использования тайных кибервозможностей. В таких случаях предварительное уведомление могло бы создать риск раскрытия информации о секретных возможностях и подорвать эффективность самих контрмер, о которых идет речь. Однако любое решение о применении контрмер без предварительного уведомления должно быть необходимым и пропорциональным цели принуждения государства к выполнению своих обязательств в этих обстоятельствах.

МЕЖДУНАРОДНОЕ ПРАВО В ОБЛАСТИ ПРАВ ЧЕЛОВЕКА

20. Обязательства, касающиеся прав человека, применимы к деятельности государств в киберпространстве, так же как и к иной деятельности. Великобритания продолжает поддерживать позицию, изложенную в Резолюции 20/8 Совета по правам человека о том, что «те же права, которые человек имеет в офлайновой среде, должны так же защищаться и в онлайновой среде...». Государства обязаны действовать в соответствии с применимыми нормами международного права в области прав человека, в том числе обычного международного права, и международных конвенций, участниками которых они являются, таких как Международный пакт о гражданских и политических правах, другие договоры ООН и региональные инструменты, такие как Европейская конвенция по правам человека.

21. Уважение государствами своих обязательств, касающихся прав человека, в отношении их поведения в киберпространстве имеет большое значение для обеспечения открытой, безопасной, стабильной, доступной и мирной среды; при этом некоторые права могут быть особенно актуальны в контексте действий государств в киберпространстве, включая право человека не подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь или произвольным и незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции, право на свободу мысли, совести и религии и право на свободное выражение своего мнения.

МЕЖДУНАРОДНОЕ ГУМАНИТАРНОЕ ПРАВО (МГП)

22. МГП применимо к операциям в киберпространстве, проводимым в осуществление враждебных действий в ходе вооруженного конфликта, так же как и к другим военным операциям.

23. МГП направлено на ограничение последствий вооруженного конфликта: оно защищает лиц, которые не принимают или больше не принимают участия в военных действиях, и ограничивает методы и средства ведения войны, применяемые участниками конфликта. Как указано выше, обращение к применению силы в киберпространстве регулируется иными нормами международного права, помимо МГП, в частности Уставом ООН. МГП направлено на ограничение последствий вооруженного конфликта, и потому было бы некорректно утверждать, что применимость его норм к кибероперациям в ходе вооруженного конфликта поощряет милитаризацию киберпространства.

24. Кибероперация может представлять собой «нападение» согласно нормам МГП, если она имеет такие же или аналогичные последствия, как и действия с использованием кинетических средств, которые квалифицировались бы как нападение. Если операция в киберпространстве признается «нападением», принципы индивидуализации, пропорциональности, гуманности и военной необходимости применимы к ней так же, как и к нападению с использованием других средств. Лица, ответственные за планирование нападений, принятие решений об их осуществлении или за их осуществление, непременно должны принимать решения на основе своей оценки информации из всех источников, которая разумно имеется у них в наличии в соответствующее время. Все соответствующие нормы МГП должны быть соблюдены при планировании и проведении операций, будь то с применением кибернетических или иных средств: сложность кибероперации не оправдывает использования более низкого стандарта защиты, обеспечиваемой для гражданского населения или гражданских объектов.

25. Гражданские лица пользуются защитой от нападения, за исключением случаев и на такой период, пока они принимают непосредственное участие в военных действиях. В той мере, в которой гражданские лица осуществляют кибероперации в ходе вооруженного конфликта, который признается нападением, они могут потерять свой статус лиц, пользующихся защитой согласно МГП, и, в силу непосредственного участия в военных действиях, становятся законными военными целями.

ЗАГЛЯДЫВАЯ ВПЕРЕД

26. Как указано выше, Соединенное Королевство Великобритании и Северной Ирландии, приветствует эту инициативу как часть продолжающегося сотрудничества между государствами, направленного на развитие взаимопонимания в отношении применимости норм международного права к поведению в киберпространстве и на укрепление их способности достигнуть этой цели.

27. Великобритания продолжит активно взаимодействовать с другими государствами, чтобы обеспечить четкое понимание в отношении применимости норм международного права к поведению в киберпространстве и параметров ответственного поведения в киберпространстве. В этой связи будет важно выйти за рамки обсуждения общих концепций и принципов и четко определить, что представляет собой противоправное поведение в

секторах, являющихся наиболее уязвимыми перед лицом деструктивного поведения в киберпространстве.

***

INTRODUCCIÓN

1. El derecho internacional es una herramienta fundamental para garantizar la estabilidad y la seguridad en el ciberespacio y es aplicable tanto con respecto a la conducta de los Estados en el ciberespacio como con respecto a sus otras conductas. La comunidad internacional reconoce claramente su aplicabilidad en la conducta de los Estados en el ciberespacio. En el reciente informe del GTCA de 2021, los Estados reafirman la interpretación (tal y como queda expresado en los informes del GEG de 2013 y 2015) de que "el derecho internacional, y en particular la Carta de las Naciones Unidas, es aplicable y esencial para mantener la paz y la estabilidad, así como para promover un contexto de las TIC que sea pacífico, accesible, estable, seguro y abierto."

2. El Reino Unido celebra por consiguiente la presente iniciativa que incita a los Estados a que presenten declaraciones que sean adjuntadas al informe del Grupo de Expertos Gubernamentales expresando su posición nacional con respecto a cómo el derecho internacional es aplicable en el ámbito del ciberespacio. Los Estados podrán gracias a estas aportaciones promover un mejor entendimiento del derecho internacional y sus avances facilitando mayor transparencia y entendimiento mutuo acerca de todo aquello que constituye un comportamiento aceptable en el ciberespacio. Mientras mayor sea la claridad de los límites del comportamiento lícito, menores los riesgos de cometer errores de cálculo y más claras las consecuencias por traspasarlos. La presente declaración se presenta como aportación a dicha iniciativa y explica brevemente, y de forma no exhaustiva, la posición del Reino Unido con respecto a todo un conjunto de asuntos concretos relativos a la forma como el derecho internacional es aplicable ante la conducta de los Estados en el ciberespacio.

3. El Reino Unido expresa su firme compromiso con la existencia de un ciberespacio seguro, pacífico, abierto y libre. Su uso es asimismo de interés para los Estados y para la comunidad internacional en su conjunto, contando aquéllos con el derecho de hacer uso de su capacidad cibernética, habida cuenta de las restricciones que imponga el derecho internacional. Si bien no existe una definición acordada a nivel internacional para definir el significado de "ciberespacio", a efectos de la presente declaración se emplea para referirse a la esfera de acciones y conductas que se realizan empleando la red interdependiente de infraestructuras de las tecnologías de la información incluido Internet, redes de telecomunicaciones relacionadas con Internet, sistemas informáticos y dispositivos conectados a Internet[278]. En la presente declaración el uso del prefijo "ciber" hace referencia a aquellas acciones que se lleven a cabo empleando las infraestructuras de la tecnología de la información antes mencionadas.

[278] Definición basada principalmente en la descripción de ciberespacio que aparece en HMG's National Cyber Security Strategy 2016-2021 [Estrategia 2016-2021 del Gobierno británico en materia de seguridad cibernética nacional], cuyo enlace aparece a continuación: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643420/Spanish_translation_-_National_Cyber_Security_Strategy_2016.pdf donde se define el ciberespacio como "la red interdependiente de infraestructuras de tecnología de la información que incluye a Internet, las redes de telecomunicaciones, los sistemas informáticos, los dispositivos interconectados y los controladores y procesadores integrados. También puede aludirse al mundo virtual o dominio como un fenómeno experimentado, o concepto abstracto."

LA CARTA DE LAS NACIONES UNIDAS

4. La Carta de las Naciones Unidas es aplicable para la conducta de los Estados en el ciberespacio, al igual que con respecto a sus otras conductas.

5. El artículo 2(4) de la Carta de las Naciones Unidas prohíbe la amenaza o el uso de la fuerza contra la integridad territorial o la independencia política de los Estados, o en cualquier otra forma que sea incompatible con los objetivos de las Naciones Unidas. Dependiendo de los hechos y circunstancias de cada caso, la conducta de los Estados en el ciberespacio puede constituir una amenaza o uso de fuerza si dicha conducta o amenaza de conducta tiene o pudiera tener el mismo efecto, o efecto similar, que mediante el empleo de medios cinéticos. En virtud del derecho internacional las circunstancias bajo las que el uso de la fuerza o la amenaza de dicho uso no incurren en la ilegalidad son las mismas independientemente de si la conducta tiene lugar de forma cinética o cibernética.

6. Una operación con medios cibernéticos puede constituir una agresión armada dando pie al derecho inherente de legítima defensa individual o colectiva, tal y como queda expresado en el artículo 51 de la Carta de las Naciones Unidas, cuando la escala y los efectos de una operación sean equivalentes a los de un ataque armado en el que se empleen medios cinéticos. Al considerar la escala y los efectos de un ataque, los factores a tener en cuenta pueden incluir la destrucción de propiedad, daños y muertes, ya sean de facto o anticipados. El ejercicio del derecho inherente de legítima defensa ante un ataque inminente o continuado ya sea efectuado con medios cinéticos o cibernéticos, puede también llevarse a cabo empleando para ello medios cinéticos o cibernéticos, cumpliendo siempre con los debidos requisitos de necesidad y proporcionalidad. El recurso al derecho inherente de legítima defensa será siempre debidamente sopesado teniendo en cuenta todas las circunstancias.

7. Tanto el artículo 2(3) como las disposiciones del Capítulo VI de la Carta sobre el arreglo pacífico de controversias pueden aplicarse igualmente con respecto a las actividades de los Estados en el ciberespacio. Por lo tanto y en virtud del artículo 33 (1), todo Estado parte de una controversia internacional de índole cibernética cuya continuación pueda poner en peligro la seguridad y la paz internacionales, deberá intentar resolver dicha disputa por medios pacíficos tal y como queda expresado en el artículo 33 de la Carta: mediante la negociación, la investigación, la mediación, la conciliación, el arbitraje, el arreglo judicial, el recurso a organismos o acuerdos regionales, u otros medios pacíficos de su elección.

NO INTERVENCIÓN Y SOBERANÍA

8. Por debajo del umbral de la amenaza o el uso de la fuerza, la norma de derecho internacional consuetudinario que prohíbe intervenciones en asuntos nacionales de los Estados es aplicable tanto a las operaciones de los Estados en el ciberespacio como lo es con respecto a sus demás actividades. Tal y como quedó expresado en la sentencia de la Corte Internacional de Justicia en el caso de Nicaragua, el objetivo de la norma de no intervención es asegurar que los Estados no sufran intervenciones coercitivas exteriores en asuntos que afecten los poderes de un Estado, cuando se trata de elementos centrales de su soberanía tales como son la libertad de elegir el sistema cultural, económico, social, o político[279].

9. De conformidad con lo expresado anteriormente por el Reino Unido, y si bien los límites precisos de esta norma siguen siendo objeto de debate, cabe señalar que presenta unas bases claramente asentadas en el marco del derecho internacional a fin de evaluar la legalidad de la conducta de un Estado. El uso de operaciones cibernéticas hostiles para manipular el sistema electoral de otro Estado con el fin de alterar los resultados de unas elecciones, así como socavar la estabilidad de su sistema financiero, o actuar contra los servicios médicos esenciales de otro Estado podrían, por lo tanto, dependiendo de las circunstancias, incumplir la prohibición del derecho internacional en materia de intervenciones.

10. La Corte Internacional de Justicia ha determinado que son consideradas intervenciones prohibidas todas aquellas que afectan a asuntos en los que cada Estado puede, en virtud del principio de soberanía de los Estados, decidir de forma libre. La soberanía como principio general es un concepto fundamental en el derecho internacional. Habida cuenta de lo anterior, el Reino Unido recuerda que toda prohibición de las actividades de los Estados ya sea en relación con el ciberespacio u otros asuntos, deberá estar claramente establecida en el derecho internacional consuetudinario o en un tratado vinculante para los Estados implicados. El Reino Unido no considera que el concepto general de soberanía constituya en sí una base clara o suficiente que permita extrapolar una norma concreta o incorporar una prohibición adicional de conducta cibernética que vaya más allá de la no intervención antes mencionada. De igual forma, el Reino Unido señala que puntos de vista divergentes sobre estos asuntos no deberían impedir que los Estados puedan evaluar si situaciones concretas constituyen actos internacionales ilícitos y llegar a conclusiones comunes con respecto a dichos asuntos.

[279] Actividades militares y paramilitares en Nicaragua y contra Nicaragua (Nicaragua contra los Estados Unidos de América) Méritos, Fallo, Informes de la CIJ 1986, parágrafo 205: ‘En este sentido [la Corte] indica que, habida cuenta de las formulaciones generalmente aceptadas, el principio prohíbe a todos los Estados o grupos de Estados intervenir de forma directa o indirecta en los asuntos internos o externos de otros Estados. Una intervención prohibida deberá ser por lo tanto aquella que afecta a cuestiones que cada Estado puede, en virtud del principio de soberanía de los Estados, decidir libremente. Una de ellas es la elección de un sistema cultural, social, económico, o político, así como la formulación de su política exterior. Una intervención es ilícita cuando emplea métodos de coerción con respecto a dichas decisiones, que deben seguir siendo libres. El elemento de coerción que define, y de hecho es la esencia de la intervención ilegal, es evidente en casos en que la intervención emplee la fuerza, ya sea de forma directa mediante acción militar, o de forma indirecta apoyando actividades armadas terroristas o subversivas en otro Estado.”

RESPONSABILIDAD DEL ESTADO Y ATRIBUCIÓN

11. El derecho internacional hace responsables a los Estados de toda actividad cibernética que les sea atribuible, en virtud de las normas de responsabilidad de los Estados. La responsabilidad de un Estado con respecto a actividades que tengan lugar en su territorio, incluidas aquellas relacionadas con actividades en el ciberespacio está por lo tanto determinada en función de las normas de derecho internacional de responsabilidad del Estado. Al igual que es responsable por los actos de sus órganos y agentes, en virtud del derecho internacional la responsabilidad también recae sobre dicho Estado cuando, por ejemplo, un individuo o grupo de individuos actúa bajo sus instrucciones o bajo su control o dirección.

12. La norma 13 (c) del Grupo de Expertos Gubernamentales de las Naciones Unidas establece que los Estados no deberán permitir a sabiendas que su territorio sea utilizado para cometer actos ilícitos internacionales utilizando las tecnologías de la información y las comunicaciones. Dicha norma incorpora orientaciones acerca de todo aquello que puede constituir comportamiento adecuado por parte de un Estado. El Reino Unido reconoce la importancia de que los Estados tomen medidas apropiadas, razonablemente disponibles, y que puedan ser llevadas a la práctica dentro de sus posibilidades para hacer frente a actividades que sean consideradas perjudiciales, con el fin de lograr una mayor estabilidad del ciberespacio en interés de todos los Estados. Cabe señalar que cuando los Estados se refieren a esta norma como no vinculante, queda patente que no existe aún una práctica de los Estados suficiente para crear una norma de derecho internacional consuetudinario de "diligencia debida" que sea aplicable a las actividades en el ciberespacio.

13. El término "atribución" se emplea con relación al ciberespacio tanto en un sentido jurídico como no jurídico. En el primero de los casos se utiliza para aludir a la identificación de aquellos individuos responsables de un acto ilícito internacional. También se emplea en un sentido no jurídico para describir la identificación de autores (incluidos actores no estatales) que hayan llevado a cabo conductas cibernéticas que podrían ser consideradas hostiles o de uso malintencionado, pero sin que impliquen necesariamente la comisión de un acto ilícito internacional.

14. Para el Reino Unido existen consideraciones diplomáticas y técnicas a tener en cuenta al atribuir públicamente dichas actividades en el ciberespacio. La decisión de hacer pública esa atribución mediante una declaración es un tema de política. Cada caso será estudiado según sus méritos. El Reino Unido hará públicas esas atribuciones de conducta con el fin de ahondar en su compromiso en pro de la claridad y la estabilidad en el ciberespacio, o cuando sea de su interés hacerlo.

15. Independientemente de la naturaleza de la atribución, no existe una obligación jurídica general que requiera que un Estado exponga públicamente la información subyacente en que basa su decisión de atribuir cierta conducta.

CONTRAMEDIDAS

16. En aras de responder a actos ilícitos internacionales, y en virtud del derecho internacional, se podrá recurrir a la adopción de contramedidas relacionadas con actividades de los Estados en el ciberespacio al igual que con respecto a otras actividades. Se entiende por ello tanto recurrir a contramedidas dirigidas hacia un Estado cuyas actividades cibernéticas constituyan actos ilegales internacionales como adoptar contramedidas mediante operaciones cibernéticas. Las contramedidas no han de ser simétricas: aun cuando el acto ilegal internacional no sea una

actividad cibernética, la respuesta sí podrá incluir contramedidas basadas en el ciberespacio (y viceversa).

17. Los Estados lesionados podrán únicamente tomar contramedidas contra un Estado responsable de cometer un acto ilegal internacional para poder hacer que dicho Estado cumpla con sus obligaciones. Toda medida adoptada deberá ser proporcional con el perjuicio causado. Las contramedidas podrán solamente llevarse a cabo de acuerdo con las condiciones y restricciones que brinda el derecho internacional y no deberán contravenir la prohibición de la amenaza o el uso de la fuerza, deberán asimismo ser necesarias y proporcionales con el objetivo de inducir al Estado responsable a que cumpla con sus obligaciones, y no deberán contravenir ninguna otra norma imperativa de derecho internacional.

18. Cuando se aplica el derecho internacional al uso de contramedidas en el ciberespacio, habrá que tener en cuenta la naturaleza de las actividades cibernéticas, que pueden comenzar y cesar de forma casi instantánea o producirse en un marco de tiempo breve. En esos casos, un patrón más amplio de actividades cibernéticas podría constituir conjuntamente un acto ilegal internacional que justifique una respuesta.

19. El Reino Unido no considera que aquellos Estados que tomen contramedidas estén obligados legalmente a dar notificación previa (incluida la solicitud de que el Estado responsable del acto ilegal internacional cumpla con el derecho internacional) en todas las circunstancias. La notificación previa puede no ser una obligación legal al responder a una intrusión cibernética encubierta empleando contramedidas, o cuando se recurre a contramedidas que dependen de capacidades cibernéticas encubiertas. En estos casos, la notificación previa podría exponer capacidades altamente sensibles y afectar la eficiencia de las contramedidas en cuestión. Aun así, toda decisión de emplear contramedidas sin dar notificación previa deberá realizarse de forma necesaria y proporcional, acorde con el objetivo de inducir al debido cumplimiento dadas las circunstancias.

DERECHO INTERNACIONAL DE LOS DERECHOS HUMANOS

20. Las obligaciones en materia de derechos humanos son aplicables tanto a las actividades de los Estados en el ciberespacio como a sus otras actividades. El Reino Unido sigue compartiendo el punto de vista expresado en la resolución 20/8 del Consejo de Derechos Humanos de que “los mismos derechos que tienen las personas en el mundo no virtual, deberán también estar protegidos en Internet…”. Los Estados tienen la obligación de actuar de forma acorde con las normas internacionales de derechos humanos, incluido el derecho internacional consuetudinario, así como con las convenciones internacionales de las que sean parte, tales como el Pacto Internacional de Derechos Civiles y Políticos, demás tratados de las Naciones Unidas, e instrumentos regionales tales como la Convención Europea de Derechos Humanos.

21. En aras de asegurar un entorno pacífico, estable, seguro, accesible y abierto es esencial que los Estados respeten sus obligaciones en materia de derechos humanos en el ciberespacio. Algunos derechos pueden estar estrechamente relacionados con ciertas actividades de los Estados en Internet tales como el derecho a no sufrir interferencias ilegales o arbitrarias en materia de privacidad, familiares, en el hogar o en la correspondencia, el derecho a la libertad de pensamiento, conciencia y religión, así como el derecho a la libertad de expresión.

DERECHO INTERNACIONAL HUMANITARIO (DIH)

22. El DIH cubre operaciones en el ciberespacio realizadas para apoyar hostilidades en conflictos armados de igual forma que es aplicable en otras operaciones militares.

23. El DIH tiene como objetivo limitar los efectos de los conflictos armados, protege a aquellas personas que, o bien no son, o bien han dejado de ser, participantes en hostilidades, y limita asimismo los métodos y medios de guerra que emplean los beligerantes. Como se indica anteriormente, el recurso al uso de la fuerza en el ciberespacio se rige por el derecho internacional, aparte del DIH, y en concreto la Carta de las Naciones Unidas. El DIH pretende limitar los efectos de los conflictos armados y es por lo tanto incorrecto afirmar que su aplicabilidad a las operaciones cibernéticas en los conflictos armados promovería la militarización del ciberespacio.

24. En virtud del DIH, toda operación cibernética puede ser considerada “ataque” cuando tenga el mismo efecto o efectos similares a los de una acción cinética considerada ataque. En aquellos casos en que una operación en el ciberespacio constituye un “ataque”, los principios de humanidad, proporcionalidad, distinción y necesidad militar son aplicables de igual forma que en ataques en los que se emplee otro tipo de medio. Aquellas personas responsables de la planificación, de la toma de decisiones o de ejecutar ataques tendrán que tomar decisiones basándose en la evaluación de la información proveniente de todas las fuentes que puedan serles razonablemente disponibles en el momento relevante. En la planificación y al llevar a cabo operaciones, ya sea por vía cibernética o de otro tipo, deberán cumplirse todas las normas pertinentes del DIH sin que la complejidad de las operaciones cibernéticas sea excusa para reducir los estándares de protección hacia civiles y objetos civiles.

25. Los civiles están protegidos de ataques salvo si participan directamente en las hostilidades y mientras dure tal participación. Al llevar a cabo operaciones cibernéticas en un conflicto armado que puedan constituir ataques, pierden el estatus de protección que les brinda el DIH y su participación de forma directa en las hostilidades les convierte por lo tanto en objetivos militares legítimos.

EN ADELANTE

26. Habida cuenta de todo lo anterior, el Reino Unido celebra la presente iniciativa como parte de la cooperación continua entre Estados con el fin de ahondar en su entendimiento de la aplicación del derecho internacional en el ciberespacio y del fortalecimiento de sus capacidades para conseguir este fin. El Reino Unido seguirá cooperando activamente con otros Estados para asegurar claridad tanto sobre la forma como el derecho internacional se aplica en el ciberespacio, como con respecto a los parámetros de comportamiento responsable de los Estados. Para ello será importante avanzar e ir más allá del debate de conceptos y principios generales y ser claros con respecto a aquello que constituye conducta ilegal en los sectores más vulnerables ante conductas cibernéticas destructivas.

United States of America

[Original: English]

I. Introduction

The United States submits this national contribution to the 2019-21 United Nations Group of Governmental Experts (GGE) on "Developments in the Field of Information and Telecommunications in the Context of International Security." This submission addresses the application of international law to the use of information and communications technologies (ICTs) by States.

The United States seeks to build upon the views expressed in the 2013 and 2015 GGEs reports, including with respect to how international law applies to the use of ICTs. In this submission, the United States seeks to deepen understanding of the legal conclusions in these consensus GGE reports, as well as to promote transparency, by sharing U.S. views on how international law applies to the use of ICTs by States. In this submission, we highlight some basic principles of international law that apply to State behavior in cyberspace and provide, where applicable, some considerations that States may take into account when determining how such principles apply to State use of ICTs in specific situations they confront. The United States believes that fostering discussion on how States understand their existing rights and obligations under international law, including with respect to self-defense, use of force, and armed conflict, apply in cyberspace actually promotes greater predictability and reduces the risk of unintended conflict. Our prior submissions to the 2014-15 and 2016-17 GGEs the Digest of United States Practice in International Law 2014 (732-40) and Digest of United States Practice in International Law 2016 (823-26) are available at: https://www.state.gov/digest-of-united-states-practice-in-international-law/.

II. Application of International Law to Cyber Activities Involving the Use of Force

There are two related bodies of international law that are relevant to the question of how existing international law applies to ICTs and the use of force in and through cyberspace: jus ad bellum (the body of law that addresses, inter alia, uses of force triggering a State's right to use force in self-defense) and jus in bello (the body of law governing the conduct of hostilities in the context of armed conflict).[280]

A. Cyber activities and *jus ad bellum*

Both the 2013 and 2015 GGE reports recognized that the Charter of the United Nations applies to States' use of ICTs[281]. The 2015 GGE report identified a number of principles of the Charter that are of central importance, including the obligation of Member States contained in Article 2(4) regarding refraining in their international relations from the threat or use of force against the territorial integrity or political

[280] The U.S. submission to the 2014–15 GGE addressed these bodies of law in some detail. U.S. Submission to the UN Group of Governmental Experts on Developments inthe Field of Information and Telecommunications in the Context of International Security (2014-2015), pp. 2-6. This section seeks only to highlight certain elements of our views.

[281] 2013 GGE Report, para. 19; 2015 GGE Report, para. 28(c).

independence of any State[282]. The 2015 GGE report also noted the inherent right of States to take measures consistent with international law and as recognized in the Charter[283]. Article 51 of the Charter recognizes "the inherent right of individual or collective self-defense" in response to an armed attack against a Member State.

1. Use of force

Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law. In determining whether a cyber activity constitutes a use of force prohibited by Article 2(4) of the UN Charter and customary international law or an armed attack sufficient to trigger a State's inherent right of self-defense, States should consider the nature and extent of injury or death to persons and the destruction of, or damage to, property. Although this is necessarily a case-by-case, fact-specific inquiry, cyber activities that proximately result in death, injury, or significant destruction, or represent an imminent threat thereof, would likely be viewed as a use of force / armed attack. If the physical consequences of a cyber activity result in the kind of damage that dropping a bomb or firing a missile would, that cyber activity should equally be considered a use of force / armed attack.

Some of the factors States should evaluate in assessing whether an event constitutes an actual or imminent use of force / armed attack in or through cyberspace include the context of the event, the actor perpetrating the action (recognizing the challenge of attribution in cyberspace, including the ability of an attacker to masquerade as another person/entity or manipulate transmission data to make it appear as if the cyber activity was launched from a different location or by a different person), the target and its location, the effects of the cyber activity, and the intent of the actor (recognizing that intent, like the identity of the attacker, may be difficult to discern, but that hostile intent may be inferred from the particular circumstances of a cyber activity), among other factors.

2. Inherent right of self-defense

A State's inherent right of self-defense, recognized in Article 51 of the UN Charter, may in certain circumstances be triggered by cyber activities that amount to an actual or imminent armed attack. This inherent right of self-defense against an actual or imminent armed attack in or through cyberspace applies whether the attacker is a State actor or a non-State actor. There is no requirement that a State defend itself using the same capabilities with which it is being attacked. States may employ cyber capabilities that rise to the level of a use of force as a means of self-defense against a kinetic armed attack (*i.e.*, one that was not launched in or through cyberspace). Additionally, States may in certain circumstances use kinetic military force in self-defense against an armed attack in or through cyberspace.

The use of force in self-defense must be limited to what is necessary and proportionate to address the imminent or actual armed attack in or through cyberspace. Before resorting to forcible measures in self-defense against an actual or imminent armed attack in or through cyberspace, States should consider whether passive cyber defenses or active defenses below the threshold of the use of force would be sufficient to neutralize the armed attack or imminent threat thereof.

[282] 2015 GGE Report, para. 26.

[283] 2015 GGE Report, para. 28(c).

B. Cyber activities and *jus in bello*

The 2015 GGE report recognized the applicability of the established jus in bello principles of humanity, necessity, proportionality, and distinction in cyberspace[284]. The applicability of the jus in bello more broadly to States' use of ICTs has been reaffirmed by a large number of Member States[285].

The United States recognizes that cyber activities in the context of an armed conflict may in certain circumstances constitute an "attack" for purposes of the application of the *jus in bello* rules that govern the conduct of hostilities, including the principles of humanity, necessity, proportionality, and distinction recognized in the 2015 GGE report.

The United States has also elaborated on *how* these principles would apply to cyber capabilities under an armed conflict. For example, the principle of distinction requires that only legitimate military objectives be made the object of attack. In the context of cyber capabilities used in armed conflict, the principle of distinction requires that only legitimate military objectives be made the object of attack.

The principle of proportionality prohibits attacks that may be expected to cause incidental loss to civilian life, injury to civilians, or damage to civilian objects which would be excessive in relation to the concrete and direct military advantage anticipated. In the cyber context, this rule would require parties to a conflict to assess the potential effects of cyber activities on both military and civilian infrastructure and users, including shared physical infrastructure (such as a dam or a power grid) that would affect civilians. In addition to the potential physical damage that a cyber activity may cause, such as death or injury that may result from effects on critical infrastructure, parties must assess the potential effects of a cyber attack on civilian objects that are not military objectives, such as private, civilian computers that hold no military significance but may be networked to military objectives.

In addition, when using cyber capabilities in armed conflict, States must comply with their obligations under international humanitarian law related to the protection of medical personnel and facilities. For example, medical personnel and facilities must not be knowingly attacked or unnecessarily prevented from discharging their proper functions, and parties to a conflict must take feasible precautions to reduce the

---

[284] 2015 GGE Report, para. 28(d).

[285] *See, e.g.,* Australia: International Cyber Engagement Strategy, Annex A: Australia's position on applies to State conduct in cyberspace (3 Oct. 2017), *available at*: https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/preliminary_information/foreword.html; Australia: 2019 International Law Supplement, *available at*: https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html; Finland: National Positions, International Law and Cyberspace, p.7 (2020), *available at*: https://front.un-arm.org/wp-content/uploads/2020/10/finland-views-cyber-and-international-law-oct-2020.pdf; France: Ministry of Defense, International Law Applied to Operations in Cyberspace, pp. 12-18 (Sept. 2019); Netherlands: Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, Appendix: International law in cyberspace, p. 5, *available at*: https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace; New Zealand: The Application of International Law to State Activity in Cyberspace, 1 Dec. 2020, *available at*: https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/cyber-il/ UK: Attorney General Jeremy Wright, *Cyber and International Law in the 20th Century*, 23 May 2018, *available at*: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

risk of incidental harm to the civilian population and other protected persons and objects, including medical personnel and facilities.

The United States has specifically addressed how its international humanitarian law obligations apply to cyberspace operations in the context of armed conflict in the Department of Defense's Law of War Manual, reflecting a commitment to ensure that U.S. legal obligations are understood and respected by its military[286]. Several other States have taken similar steps to share their views on how international humanitarian law applies and / or address cyber specifically in their military manuals[287].

For example, in the context of *jus ad bellum*, it is important for States to understand what types of activities would be interpreted by other States as violations of Article 2(4) or that might prompt a State to invoke its right of self-defense under Article 51. Similarly, it is important for States to develop clear understandings of the restrictions that the Charter and customary international law place on this type of conduct; for example, even where a State may lawfully use force in self-defense, its response must be necessary and proportionate to respond to an actual or imminent armed attack. The United States has sought to be transparent about its views in this regard, including through its submissions to this and previous GGEs, and would encourage other States to do the same.

Similarly, international humanitarian law regulates the conduct of hostilities to minimize their effects on civilians and avoid unnecessary suffering. It does so in part through specific protections for civilians and civilian objects. Understanding how these protections apply in the context of cyber attacks is particularly important, given the often dual-use nature of ICT infrastructure and interconnectivity of ICTs. Affirmation that this body of law applies is consistent with our common commitment to the pursuit of peace.

III. Application of International Law to Cyber Activities Below the Level of a Use of Force

A. Respect for the sovereign equality of States and human rights

As recognized in the 2013 and 2015 GGE reports, State sovereignty and the international principles that flow from sovereignty apply to States' ICT-related activities and to their jurisdiction over ICT infrastructure within their territory[288].

The United States believes that State sovereignty, among other long-standing international legal principles, must be taken into account in the conduct of activities in cyberspace. Whenever a State contemplates conducting activities in cyberspace, the equal sovereignty of other States needs to be considered.

The implications of sovereignty for cyber activities are complex, but we can start by noting two important implications of sovereignty for ICT-related activities. First, we acknowledge the continuing relevance of territorial jurisdiction, even to

[286] Department of Defense, Law of War Manual, § 16, *available at*: https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

[287] *See* note 6 *supra*; *see also* Danish Ministry of Defense, Military Manual on International Law Relevant to Danish Armed Forces in International Operations, § 3.10, *Regulation of Computer Network Operations in international law* (12 Oct. 2020), *available at*: https://forsvaret.dk/en/publications/military-manual/.

[288] 2013 GGE Report, para. 20; 2015 GGE Report, para. 27.

cyber activities, and second, we acknowledge the exercise of jurisdiction by the territorial State is not unlimited; it must also be consistent with applicable international law, including international human rights obligations.

Among other international legal principles, the 2015 GGE report acknowledges the principle of non-intervention in the internal affairs of other States [289]. As articulated by the International Court of Justice (ICJ) in its judgment on the merits in the Nicaragua Case, this rule of customary international law forbids States from engaging in coercive action that bears on a matter that each State is entitled, by the principle of State sovereignty, to decide freely, such as the choice of a political, economic, social, and cultural system. This is generally viewed as a relatively narrow rule of customary international law, but States' cyber activities could run afoul of this prohibition. For example, a cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention. Other States have made similar observations.[290] Further, a cyber operation that attempts to interfere coercively with a State's ability to protect the health of its population--for example, through vaccine research or running cyber-controlled ventilators within its territories during a pandemic--could be considered a violation of the rule of non-intervention.

In certain circumstances, one State's non-consensual cyber operation in another State's territory, even if it falls below the threshold of a use of force or non-intervention, could also violate international law. However, a State's remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a *per se* violation of international law. In other words, there is no absolute prohibition on such operations as a matter of international law. This is perhaps most clear where such activities in another State's territory have no effects or *de minimis* effects. The very design of the Internet may lead to some encroachment on other sovereign jurisdictions.

Finally, while the physical infrastructure that supports the Internet and cyber activities is generally located in sovereign territory and is subject to the jurisdiction of the territorial State, the exercise of jurisdiction by the territorial State is not unlimited. It must be consistent with applicable international law, including international human rights obligations. The 1948 Universal Declaration of Human Rights (UDHR) says: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[291]

---

[289] 2015 GGE Report, para. 26.

[290] *See, e.g.,* Australia: 2019 International Law Supplement, *available at*: https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html; Estonia: President Kersti Kaljulaid, Opening Speech at Cybercon, 29 May 2019, *available a*t: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html; Finland: National Positions, International Law and Cyberspace, p. 3 (2020), *available at*: https://front.un-arm.org/wp-content/uploads/2020/10/finland-views-cyber-and-international-law-oct-2020.pdf; New Zealand: The Application of International Law to State Activity in Cyberspace, 1 Dec. 2020, *available at*: https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/cyber-il/ UK: Attorney General Jeremy Wright, *Cyber and International Law in the 20th Century*, 23 May 2018, *available at*: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

[291] Universal Declaration of Human Rights, UN General Assembly, 217 A (III) (Dec. 10, 1948), art. 19 (UHDR) (emphasis added).

All human beings hold certain rights, whether they choose to exercise them in a city square or an Internet chat room. The right to freedom of expression is well-established internationally in both the UDHR and the International Covenant on Civil and Political Rights.[292] Both of these instruments clearly state that this right can be exercised through any media and regardless of frontiers. Both of these instruments set forth the right of individuals to publish, to create art, to practice their religions, and to gather together and discuss issues of the day. Regardless of whether these activities occur online or offline, they are governed by the same principles.

B. The Concept of "Due Diligence"

In recent public statements on how international law applies in cyberspace, a few States have referenced the concept of "due diligence": that States have a general international law obligation to take steps to address activity emanating from their territory that is harmful to other States, and that such a general obligation applies more specifically, as a matter of international law, to cyber activities. The United States has not identified the State practice and opinio juris that would support a claim that due diligence currently constitutes a general obligation under international law. We do believe, however, that if a State is notified of harmful activity emanating from its territory it must take reasonable steps to address such activity.

C. State responsibility for internationally wrongful acts

Both the 2013 and 2015 GGE reports concluded that States must meet their international obligations regarding internationally wrongful acts attributable to them under international law.[293] In addition, they must not use proxies to commit internationally wrongful acts using ICTs.[294]

Under the law of State responsibility, a State is responsible for an internationally wrongful act when there is an act or omission that is attributable to it under international law that constitutes a breach of an international obligation of the State. Cyber activities may therefore constitute internationally wrongful acts under the law of State responsibility if they are inconsistent with an international obligation of the State and are attributable to it.

The law of State responsibility supplies the standards for attributing acts, including cyber acts, to States. For example, cyber operations conducted by organs of a State or by persons or entities empowered by domestic law to exercise elements of governmental authority are attributable to that State. As important, as a legal matter, States cannot escape responsibility for internationally wrongful cyber acts by perpetrating them through proxies; cyber operations conducted by non-State actors are attributable to a State under the law of State responsibility when such operations are engaged in pursuant to the State's instructions or under the State's direction or control, or when the State later acknowledges and adopts the operations as its own. Thus, when there is information—whether obtained through technical means or all-source intelligence—that permits attribution of a cyber act of an ostensibly non-State actor to a State under the international law of State responsibility, the victim State has

[292] UDHR, art. 19; International Covenant on Civil and Political Rights, UN Treaty Series 999, 171, art. 19.

[293] 2013 GGE Report, para. 23; 2015 GGE Report, para. 28(f)

[294] 2013 GGE Report, para. 23; 2015 GGE Report, para. 28(e).

all of the rights and remedies against the responsible State permitted to it under international law.

The law of State responsibility does not set forth burdens or standards of proof for attribution. Such questions may be relevant for judicial or other types of proceedings, but they do not apply as an international legal matter to a State's determination about attribution of internationally wrongful cyber acts for purposes of its response to such acts, including by taking unilateral, self-help measures permissible under international law, such as countermeasures. In that context, a State acts as its own judge of the facts and may make a unilateral determination with respect to attribution of a cyber operation to another State. Absolute certainty is not required. Instead, international law generally requires that States act reasonably under the circumstances. Similarly, there is no international legal obligation to reveal evidence on which attribution is based. But to facilitate global understanding of emerging state practice in this rapidly developing area, public attributions should, wherever feasible, include sufficient evidence to allow corroboration or cross-checking of allegations.

Attribution plays an important role in States' responses to malicious cyber activities as a matter of international law. It is crucial, however, to distinguish legal attribution from attribution in the technical and political senses. States and commentators often express concerns about the challenge of attribution in a *technical* sense—that is, the challenge in light of certain characteristics of cyberspace of obtaining facts, whether through technical indicators or all-source intelligence, that would inform a State's policy and legal determinations about a particular cyber incident. Others have raised issues related to *political* decisions about attribution—that is, considerations that might be relevant to a State's decision to go public and identify another State as the actor responsible for a particular cyber incident and to condemn a particular cyber act as unacceptable. As norms emerge to clarify how international law addresses the issue of attribution, it would be useful, wherever possible, for law-abiding states to share information regarding both technical knowhow and state practice.

D. Countermeasures and Retorsions

In certain circumstances, a State injured by cyber activities that are attributable to another State and that constitute an internationally wrongful act, but do not amount to an armed attack, may respond with non-forcible countermeasures [295]. Such countermeasures must be directed only at the State responsible for the wrongful act, must meet the requirements of necessity and proportionality, must be designed to induce the State to return to compliance with its international obligations, and, under the customary international law of State responsibility, must be suspended without undue delay if the internationally wrongful act has ceased.

Before an injured State can undertake countermeasures in response to a cyber-based internationally wrongful act attributable to a State, it generally must call upon the responsible State to cease its wrongful conduct, unless urgent countermeasures are necessary to preserve the injured State's rights. The sufficiency of this prior demand on the responsible State should be evaluated on a case-by-case basis in light of the particular circumstances of the situation at hand and the purpose of the requirement, which is to give the responsible State notice of the injured State's claim and an opportunity to respond. Countermeasures taken in response to cyber activities

[295] Countermeasures are acts that would otherwise be contrary to the international obligations of an injured State vis-à-vis the responsible State if they were not taken in response to an internationally wrongful act by the latter in order to procure cessation.

attributable to States that constitute internationally wrongful acts may take the form of cyber-based countermeasures or non-cyber-based countermeasures.

Countermeasures are distinct from acts of retorsion, which are unfriendly acts that are not inconsistent with any international obligations. Acts of retorsion may include the imposition of sanctions or the declaration that a diplomat is *persona non grata*. A State can always undertake such responsive measures that are not inconsistent with any of its international obligations in order to influence the behavior of other States, including in response to destabilizing cyber activities.