Appendix: International law in cyberspace

This is a translation of a document sent by the Government of the Kingdom of the Netherlands to Parliament. No rights can be derived from this version, the original text is authoritative.

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.[1]

As the government has indicated on multiple occasions and consistently argues, international law is applicable in cyberspace. This is also recognised internationally.[2] 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.

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.[3] 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.

---

[1] 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.

[2] 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.

[3] *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.'

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.[4] 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 obligations and 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, human and 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 enforce the 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 cyber operations that violate the sovereignty of another country. It should be noted in this regard that the precise 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 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 activities performed 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 thus violates 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

[4] *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.

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.[5] 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 law sets 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 from which 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 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 crystallised in 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.[6]

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.[7] 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

[5] 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.

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

[7] 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 9.

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 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.'*[8] 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.[9] 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,*[10] 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 respect of cyber activities:

- carried out by persons in their territory or where use is made of items or networks that are 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.[11]

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 cyber activity in question is carried out by a state or non-state actor, or where this actor is located. If, for example, a cyberattack is 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.

---

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

[9] *Tallinn Manual 2.0,* Rule 69.

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

[11] *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.

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 depends on 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'.[12]

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.*'[13]

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.[14] 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 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 the privacy 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 under certain 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 limited period. 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

[12] '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.

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

[14] 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.

Assembly, among others.[15] However, it is clear that ongoing digitalisation and technological advances are raising new questions and presenting new challenges when it comes to the application of 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 via online 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 instruments provides 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 draw attention 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 advent of social media, as have the right to education and the right to health, given the wealth of information and 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 and free 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,[16] 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 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 of a 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.

[15] 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).

[16] For a discussion of countermeasures see page 8 of this appendix.

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.'*[17]

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 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 involved in 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.[18] 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;

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

[18] 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;[19]
- 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 which the 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 aimed at 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 community as 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.[20] 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.[21] 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.

To determine whether an operation constitutes an armed attack, the scale and effects of the operation must be considered.[22] 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

[19] 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.

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

[21] The term 'prohibition of the use of force' is explained on page 3.

[22] *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.

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.[23]

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.'*[24] 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 invoking the 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.'*

[23] Ibid.

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