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.

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

During the plenary parliamentary debate of 20 December 2018 on espionage by Russia (Proceedings of the House of Representatives, 2018-2019, no. 39, item 33), the government undertook to provide an overview of the application in cyberspace of relevant elements of existing international law. In addition, a motion submitted by MPs Kees Verhoeven and Hanke Bruins Slot (Parliamentary Paper 33 694, no. 35) requested an overview of initiatives aimed at strengthening the international legal order in cyberspace. I am writing in conjunction with the Ministers of Defence, Justice and Security, and the Interior and Kingdom Relations to inform the House regarding the above issues. The enclosed appendix discusses the main issues relating to international law.

Strengthening the international legal order in cyberspace

The government aims to play a leading role in the application and strengthening of an international normative framework for the regulation of cyber operations between states. The cyber sanctions regime initiated by the Netherlands and recently adopted by the EU is an example of Dutch efforts in this area. The framework will largely be rooted in existing international law. After all, the Netherlands benefits from a well-functioning international legal order that provides a measure of predictability, stability and conflict prevention.

As explained in the 2019 Cybersecurity Assessment for the Netherlands[1] and the annual reports of the intelligence and security services,[2] the cyber threat posed by state actors is increasing, and there is insufficient consensus about what international standards and values apply in cyberspace. Recent incidents, such as the disruption on 13 April 2018 of a Russian military intelligence (GRU) cyber operation targeting the Organisation for the Prohibition of Chemical Weapons (OPCW), are one manifestation of a much broader geopolitical trend. The status quo is increasingly being threatened by state actors seeking to exploit the vulnerabilities inherent in digitalisation.

In order to provide guidance specifically tailored to cyberspace, the government is also pressing for international agreements on voluntary, non-binding norms of behaviour by states and the development of a system of confidence-building measures. The 2010, 2013 and 2015 consensus reports of the UN Group of Governmental Experts form the basis for these efforts.[3] In this way the

[1] Cybersecurity Assessment for the Netherlands (CSBN) 2019, Parliamentary Paper no. TBC.
[2] 2018 annual report (public) by the General Intelligence and Security Service (AIVD) (Parliamentary Paper 30 977,
no. 154) and 2018 annual report (public) by the Military Intelligence and Security Service (MIVD) (Parliamentary Paper 29 924, no. 184).
[3] UNGGE consensus reports, 2009/2010, A/65/201, 2012/2013, A/68/98*, 2014/2015, A/70/174.

Netherlands is contributing to the development of an international security architecture for cyberspace.

The government considers it crucial for businesses, knowledge institutions, the tech community and civil society organisations to be involved in these efforts. For this reason, in addition to the existing inter-state processes, the government has lent its support to initiatives such as the Global Commission on the Stability of Cyberspace (GCSC). This body is working to develop a framework for stability in cyberspace. Its final report will be completed in November 2019.

In the run-up to negotiations in two UN bodies,[4] the Netherlands will use consultations on the application of international law in cyberspace in its efforts to increase support for an open, free and secure internet. To this end, the government recently arranged international consultations with a large number of states on this matter.

In addition the government is working to build capacity aimed at broadening international support for an open, free and secure internet where existing international law is respected and implemented. Strategic capacity-building activities have been carried out via the Global Forum on Cyber Expertise (GFCE), which was launched by the Netherlands in 2015. The application of international law in cyberspace is one of the GFCE's focus areas. Using the Tallinn Manual 2.0, countries all over the world are now carrying out capacity-building projects.[5]

In both UN processes there will no doubt be attempts to call into question the application of international law in cyberspace and previous UN-agreed principles and norms of behaviour. Such attempts will need to be actively resisted. There is an increasingly sharp divide between multistakeholder-oriented countries (such as the Netherlands), which seek to protect the openness, freedom and integrity of the internet, and state-oriented countries that seek to control and restrict all content disseminated online. In this context the efforts of the network of Dutch diplomatic missions, which is being strengthened in the area of cyber expertise, are crucial.

Diplomatic and political response to cyber incidents

As the international debate on the application and scope of international law in cyberspace proceeds, some countries continue to engage in harmful activities. Diplomatic measures against undesirable state-led cyber operations, ideally coordinated at international level or in coalition with like-minded countries, can be an effective way to strengthen the international legal order and protect security interests at home and abroad. The government is therefore working to strengthen our capacity to mount a diplomatic and political response to cyber operations that undermine our interests. The international response after the foiled cyber operation targeting the OPCW is a good

[4] In 2019 the Netherlands is again participating in the United Nations Group of Governmental Experts (UNGGE). In addition the Netherlands will be part of the Open-ended Working Group on International Cybersecurity, which was established further to a Russian resolution in the UN General Assembly.
[5] The Netherlands supports a more inclusive and detailed debate on the application of international law to cyber operations using the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

example of this. The efforts of the mission network are essential in this respect, so as to ensure coordinated action. When assessing the options for responding, the focus above all must be on carefully and comprehensively weighing up the Netherlands' interests, including those in the realm of security.

In order to provide further structure to international cooperation at EU level, an EU cyber diplomacy 'toolbox' has been developed, at the Netherlands' initiative.[6] The toolbox is a framework which allows various instruments of the Common Foreign and Security Policy to be used to hold parties conducting harmful cyber activities to account. In this connection, on 17 May 2019 an EU cyber sanctions regime was introduced at the Netherlands' initiative, making it possible to freeze assets and impose entry bans.[7]

It is equally important for the NATO Alliance to be able to defend itself against the full spectrum of hostile cyber operations. Such operations include not only those that can be considered armed attacks, but also those that are part of a hybrid campaign that falls below the threshold of armed conflict. The government will continue to advocate to this end at NATO level.

Conclusion

The appendix sets out the main rules of international law that apply in cyberspace. It also explains the government's interpretation of the application of those rules. Where relevant, it indicates what issues are still the subject of international debate and where the rules need to be elaborated further. In this connection the appendix also discusses the obligations of states in cyberspace, the attribution of cyber operations and options for responding to undesirable cyber activity by another state.

In the meantime, the government will continue its efforts in the existing frameworks of the Integrated International Security Strategy and the Netherlands Cybersecurity Agenda. The priorities are i) strengthening the diplomatic response framework at EU and NATO level and in coalition with like-minded countries, and ii) broadening support for an open, free and secure internet where existing international law applies and is respected. The government will inform the House of its progress in mid-2020.

[6] Doc. 9916/17 Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities.
[7] Doc. 7299/19 Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States.