Resolution 69/28

Developments in the field of information and telecommunications in the context of international security

Kingdom of the Netherlands

2015

General appreciation of the issues of information security

Cyberspace and especially the Internet have fast become a critical resource for citizens, companies and governments alike. The increased importance of cyberspace has presented our global community with new challenges. As our societies become more interconnected and dependent on the Internet and ICTs, they become more vulnerable to the misuse of these technologies. This misuse is incentivized by low entry costs, high potential gains and low political and legal risks in case of discovery. Given the unique attributes of ICTs and the difficulty of verifying behavior, there is the potential for mistaken attribution, miscalculation and unintended escalation in a time of crisis.

The need for international cooperation to reduce these risks is clear. This is a strategic challenge for states that transcends the technical and operational level. It is also a challenge in which the private sector must be a part of any solution, given its ownership over most of the ICT infrastructure around the world.

In light of the above, the Netherlands is stepping up its engagement in cyber diplomacy to maintain peace and stability in cyberspace, promote the international legal order and foster a culture of collaborative security.

Efforts taken at national level to strengthen information security and promote international cooperation in the field

The Netherlands is working nationally and internationally for a secure digital environment. Cyber security is a government priority. Maintaining our ability to respond to cyber threats and provide a safe and secure digital environment for our citizens requires constant
adaptation and vigilance. However, when pursuing cyber security policies, the Netherlands’
efforts are always bound by two conditions:

- First, it is essential that fundamental human rights, including freedom of expression
  online and privacy, are safeguarded. The same rights that people have offline must also
  be protected online. The Netherlands commits itself to respect its human rights
  obligations, as well as the principles of the rule of law, legitimate purpose, non-
  arbitrariness, effective oversight, and transparency in conducting our policy actions. The
  Netherlands calls on all States to do the same.

- Second, it is important to ensure that policies aimed at increasing cyber security do not
  compromise the ability of the open internet to function as an engine for innovation and
  social and economic growth. The free flow of information and ideas has generated
  immense prosperity and progress and must be guaranteed.

In the view of the Netherlands, respect for human rights and fundamental freedoms, the
open and global nature of cyberspace and security online are complementary concepts. This
is the core of our second cyber security strategy, entitled 'National Cyber Security Strategy
2: from awareness to capability', which was published in 2013. The Netherlands regards the
multistakeholder approach to internet governance and cyber security as the most effective
approach to maintaining an open, free and secure internet.

The Netherlands has a National Cyber Security Centre, which main activities are as follows:
responding to threats and incidents, publishing perception and action prospects and
improving crisis management. The NCSC also provides a platform for cyber security
cooperation. It is a partner in several multilateral networks, such as FIRST, EGC, IWWN,
Terena, I4, ISF, and others in which information and best practices are shared.

The Dutch National Cyber Security Council, established in 2011, has continued to ensure a
collaborative approach between the public sector, the private sector and academic and
research institutions at the level of strategic decision makers in the field of cyber security.

In July 2014, the National Cyber Security Centre released its fourth comprehensive Cyber
Security Assessment, which details the Netherlands’ perception of the extent of threats to
and from cyberspace and is put together in close collaboration between public and private
parties. It concluded that the biggest threat to Dutch interests is posed by professional
criminals (due to various forms of cyber criminality) and by state actors (due to the risk of digital espionage and disruptive attacks). Measures to address these threats and improve resilience are being implemented, including the National Response Network, a public-private partnership the purpose of which is to enhance societal resilience using a joint response to cyber security incidents, and guidelines for Responsible Disclosure. The Netherlands is very willing to share these measures with third countries, for example through the Global Forum on Cyber Expertise (GFCE), which was launched during the Global Conference on Cyberspace 2015 in The Hague (see below).

One of the ways in which the Netherlands has been working towards improving international cooperation and exchange of information on cyber security, is by hosting the fourth Global Conference on Cyberspace (GCCS) in April 2015. Throughout 2014, the Netherlands supported many initiatives which contributed to the GCCS and other relevant processes. An important element of these preparations was the establishment of the Global Forum for Cyber Expertise, with the support of partner countries and private companies from around the globe.

Further, in the context of Resolution 69/28, the activities that were supported by The Netherlands include the UNIDIR International Law and State Behavior in Cyberspace Meeting Series, ICT4Peace working papers on ‘Norms for International Peace and Security’, a seminar at The Hague Centre for Strategic Studies centred around the question ‘What can and should be protected in and through cyberspace?’, a course on Cyber Diplomacy offered by the Clingendael Institute for International Relations in cooperation with ICT4peace, and a training organized by Global Partners Digital aimed at enhancing the awareness and understanding about cybersecurity issues and processes and more informed engagement by civil society actors. We furthermore supported events organised by the Asia-Pacific-based think tanks ORF and ASPI and were active participants in international dialogues to build understanding and trust, such as the Sino-European Cyber Dialogue.

In order to safeguard the deployability of the Netherlands armed forces and to increase the effectiveness of the armed forces, the ministry of Defence continued to invest in its digital resilience, including in cyber capabilities. This concerns both the capability to protect its networks and systems from attacks and the capability to take offensive measures. To this end, in 2014 a Cyber Command was formally established.

In its updated Defence Cyber Strategy, published in February 2015, the Ministry of Defense explicitly (re)states that the existing international frameworks of rules and restrictions equally
apply to cyber operations. The deployment of military cyber capabilities is subject to the same political decision making process as for conventional operations.

Relevant international concepts and possible measures that could be taken by the international community to strengthen information security at the global level

The Netherlands intends to remain an active contributor to ongoing discussions on international peace and security in cyberspace. In the view of the Netherlands, the following areas would benefit from further work and concrete measures:

1. Much work has been done to affirm the applicability in cyberspace of existing international law and norms for State conduct, in which especially the 2013 the report of the Group of Governmental Experts stands out as a landmark achievement. It confirms that there is a responsibility for States to prevent conflict in cyberspace and ensure that, if cyber capabilities are used by States, they should be used in accordance with international law, including the UN Charter. At the same time, more needs to be done to enhance States’ understanding of how these existing rules apply.

2. Of particular importance is the examination of the international legal framework that applies to cyber operations that do not rise to the threshold of an armed attack. This includes the question of how the principle of State sovereignty applies to State activities in cyberspace, consistent with States’ international obligations and the law of State responsibility. It also includes the question of the application of the principle of due diligence, i.e. not to knowingly allow a State’s territory to be used for acts contrary to the rights of other States. The international community needs to further invest in activities that lead to shared understandings of these and other obligations and responsibilities towards each other.

3. In addition to the above, the international community needs continued dialogue on the question what norms or additional measures of self-restraint or mutual assistance States and companies could implement to create a more stable cyberspace. The idea that States should establish special normative protection for certain systems and networks, including critical infrastructure providing essential civilian services, civilian incident
response structures and certain critical components of the global internet, both physical and logical, has been gaining traction for some time. How such protection could be established and which objects would be candidates to include in this category is a matter for further debate. A norm built around a “responsibility to assist” would also be recommendable.

4. There is a clear, shared interest in strengthening legal, diplomatic and policy capacity and the exchange of best practices in the field of cyber norm development and confidence building measures. Regional initiatives, such as the ASEAN Regional Forum, the Organization for Security and Cooperation in Europe, the African Union and the Organization of American States, provide an inclusive and cooperative approach to achieving this objective. These efforts should be supported and intensified.

5. States need to be transparent about the roles and responsibilities of their defence forces and security services in the cyber domain. The Netherlands sees a need to (further) pursue dialogue and other measures related to cyber issues among their defence forces and security services to build confidence and ensure international stability.

6. There is a great need to step up efforts for capacity building. At both the technical and policy level the international community needs to learn from each other and exchange best practices in various fields in cyberspace, like cyber security, data protection, cybercrime and e-governance. Concrete examples one could think of are improving the maturity of CSIRTs, the implementation of standards, awareness raising programs, data protection legislation, Responsible Disclosure and different models of public private cooperation. To contribute to this goal, the Netherlands, together with 41 other partners, launched the Global Forum on Cyber Expertise (GFCE) at the Global Conference on Cyberspace on 16 April 2015. The GFCE is open for interested partners.

7. Businesses, academia, the technical community and other civil society organisations can all make an important contribution to enhancing ongoing processes for international peace and security in cyberspace. They should be included in the continuing dialogue and encouraged to constructively contributing to strengthening international peace and security. It is equally important to expand the number of (state) actors that is able to contribute to the dialogue on cyber issues in relation to international security.