‘UN Sanctions and Digital Technologies: Threats and Opportunities’, 9 February 2016 New York

Introductory words by Dr Marja Lehto

Excellencies, distinguished speakers and participants,

Today’s topic, digital technologies and UN sanctions, may be new, but discussions on cyber threats and international law have abounded in the past 15 to 20 years, producing not only countless academic articles but also a number of attempts to lay down standards and legal obligations.

The main angles from which to look at the threats so far have been cybercrime, on the one hand, and cyber warfare, on the other**.**

Cybercrime

The first negotiated international response to cyber threats, at the regional level, was the Council of Europe Convention on Cybercrime, the so-called Budapest Convention that was adopted in 2001.

When the member states of the Council of Europe embarked on drafting this convention in 1996, they cited several reasons:

1) the emergence of new types of crime

2) The need to cover the commission of traditional crimes by means of new technologies

3) It was also noted that the consequences of criminal behaviour could be more far-reaching than before because they were not restricted by geographical limitations or national boundaries.

4) Furthermore, new technologies were seen to challenge existing legal concepts (such as jurisdiction) as criminals were increasingly located in in places other than where the effects of their acts were felt.

When adopted, the Budapest Convention was the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It is still one of the very few binding international instruments in this area, apart from the new African Union Convention on Cybersecurity and Data Protection, adopted in 2014.

The Budapest Convention aims at: 1) harmonising the domestic criminal law with regard to cyber offences and related provisions, 2) affecting domestic criminal procedural law with the view to providing sufficient powers for the investigation and prosecution of such offences (such as the search of computer networks and interception), and 3) setting up a fast and effective regime of international cooperation.

The Convention is open to non-member states of the Council of Europe and, for instance, the OAS has encouraged member states to join the Convention. It has been ratified to-date by 40 states members of the Council of Europe and eight non-member states.

Irrespective of how widely the Budapest Convention will be ratified by states outside the Council of Europe, it may serve as a model, identifying the obligations for states to enact and enforce cybercrime laws within their territories and to cooperate to prosecute or extradite cybercriminals.

Cyberwarfare

The discussion about the applicability of international law to cyber activities began around the turn of the millennium. It was for a long time almost exclusively focused on use of force and armed conflict: how to define the threshold of use of force, or the threshold of armed attack with regard to cyberwarfare, and how international humanitarian law applies in cyber space. I will therefore call it the 'cyberwarfare track', as distinct from the 'cybercrime track'.

One of the most noteworthy results of this discussion has been the 2013 Tallinn Manual on the International Law Applicable to Cyber Warfare (prepared by an International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence).

The ambition of the Tallinn Manual has been to provide a restatement of law, that is, a realistic assessment of what states regard as existing law. There are two elements in this.

First, the Manual seeks to provide an accurate picture of the law as it is, leaving aside progressive development of the law.

Secondly, and for exactly the same reason, there are open questions and areas of uncertainty, related to the relative absence of reported state practice, or to the fact that the views of states diverge on certain issues and interpretations of law.

The Tallinn Manual has been quite influential as a contribution to the discussion of cyber security. This is probably due to its specificity. The Manual goes into the substance of all essential rules that govern use of armed force by states, or the laws of armed conflict (international humanitarian law), as well as a number of other questions related to state responsibility and jurisdiction.

The first edition of the Tallinn Manual, published in 2013, covers thus a fairly restricted area of law applicable to cyberwarfare but efforts are underway to complement these rules with a much broader set of rules applicable outside of armed conflict, including sovereignty, counter-measures, intervention, diplomatic law and human rights.

It should nevertheless be stressed that the list of rules contained in the Tallinn Manual is a product of expert work, and does not represent a negotiated outcome, or geographically balanced views. I therefore turn now to the UN GGE.

UN GGE

The issue of information security has been on the UN agenda since 1998, when the first resolution on this item was adopted. The resolution stressed the need to develop international principles that would enhance the security of global information and telecommunications systems and help to combat what was then called ‘information terrorism’ and criminality.

Later there have been successive Groups of Governmental Experts to discuss existing and potential threats in the sphere of information security.

The latest UN GGE, which completed its work last year, identified a number of threats, including both the use of ICTs in future conflicts between States, and the use of ICTs for terrorist purposes such as recruitment, financing, training and incitement, or terrorist attacks against ICTs or ICT-dependent infrastructure, as well as malicious ICT actions by criminal groups or other non-State actors.

The report contains a list of basic principles of responsible state behaviour in cyberspace, for instance that states should cooperate to prevent practices that are harmful or that may pose threats to international peace and security, and prosecute terrorist or criminal use of ICTs.

***

It is quite striking that, during all these years, the topic of UN sanctions has received fairly little attention in the context of cyber threats. It is nevertheless clear that the new technologies can be used and abused for different kinds of norm-breaking activities, including those that contribute to terrorist acts or hamper the effective implementation of UN sanctions.

This is all the more relevant as we know that most sanctions regimes are affected by evasion and that the new and emerging digital technologies provide ample opportunities to disguise such activities.

It is therefore very appropriate and timely that the Compendium of the High Level Review of UN Sanctions identified abuse of internet and digital technologies as one of the ongoing and emerging challenges that need to be addressed in relation to UN sanctions. Some of the relevant issues will be specified in the three presentations we are about to hear.

The first presentation by H.E. Mr van Bohemen will shed light on the role of digital technologies with regard to the counter terrorism efforts of the UN, a theme that has been identified by the UNSC as relevant but which has not yet received a very systematic treatment.

The second presentation by Mr Carisch will focus on the technological developments that can make violations of sanctions regimes increasingly difficult to detect and to legally address.

I would like to argue that both these areas can profit from the work already done in order to promote broadly accepted standards and definitions, to harmonize national criminal legislations and to enhance international cooperation to counter cybercrime.

At the same time, further guidance would be needed on how to address the specific challenges related to certain terrorist activities or to circumventing UN sanctions with the help of new digital technologies.

And while the cybercrime track may be the most obvious source to look at for inspiration, the processes that focus on the rights and obligations of states (such as the UN GGE and the Tallinn Manual process) can also be relevant insofar as they contribute to defining standards of cybersecurity due diligence.

Without shared standards and without international cooperation security threats in cyberspace cannot be adequately addressed. And as was pointed out by the UN GGE Report last year, different levels of capacity for ICT security among States can increase vulnerability in an interconnected world.

The third presentation will be given by Mr Miguelez and Mr Greene. They will present us some of the pragmatic technological solutions that may be helpful in detecting illegal activities or facilitating the implementation of complex sanctions measures.

It has been noted that, curiously, there is a tendency to use the prefix 'cyber' with regard to security issues, crime and war, whereas other prefixes with similar content such as 'digital', 'virtual' or 'e-' seem to have more positive connotations.

I think therefore that it is appropriate to speak in this context of 'emerging digital technologies' which are seen both to pose threats and to provide solutions and opportunities.

After the three presentations there will be time for questions and answers as well as for discussion of how best to continue to explore these questions