På vei mot en global protokoll om cybersikkerhet og cyberkriminalitet

av Stein Schjølberg

Europarådets konvensjon om cybercrime fra 2001 er ratifisert eller har fått tilslutning av de fleste land i den vestlige verden. Globalt har konvensjonen ikke fått samme grad av oppslutning i andre land og regioner.

På denne bakgrunn må det reises spørsmål om behovet for en ny internasjonal avtale i FN-systemet om cyberkriminalitet. Hvilken form dette bør få er et åpent spørsmål. Hvis man ønsker en bindende konvensjon eller traktat vil dette ta mange år. Ønsker man derimot en mer løselig anbefaling som en *Recommendation* eller *Memorandum of Understanding (MoU)* gir det et kortere tidsperspektiv. En MoU er en rammeavtale som trekker opp målene og grunnlaget for en felles forståelse og intensjoner innenfor et konkret emne. Den internasjonale telekommunikasjonsunion (ITU) i Genève er den av FN-institusjonene som er best posisjonert til å lede arbeidet både med hensyn til medlemsland og funksjon.

Den globale utvikling

I oktober 2007 ble jeg ble oppnevnt av ITU som leder av en global ekspertgruppe *(High-Level Experts Group, HLEG)* med over 100 medlemmer fra mange land, internasjonale organisasjoner, universiteter og privat industri. Etter en omfattende møtevirksomhet avsluttet vi arbeidet med to rapporter. *Chairman's Report* ble offentliggjort i august 2008, mens *Global Strategic Report* ble overlevert i november 2008. Grunnlaget skal nå være lagt for et globalt rammeverk som land også utenfor Europa og den vestlige verden kan slutte seg til.

Etter mer enn 30 års arbeid med data- og cyberkriminalitet for internasjonale organisasjoner, samt en omfattende nasjonal og internasjonal utrednings- og foredragsvirksomhet, antar jeg at en slik mulighet er innen rekkevidde. Gjennom det internasjonale samarbeidet i Interpol, OECD og Europarådet trodde vi imidlertid at vi hadde nådd dette målet allerede i slutten av 1980-årene. Da Internett plutselig var der i midten av 1990-årene, forsto vi likevel at vi fortsatt bare var ved begynnelsen.

Bakgrunnen

FNs hovedforsamling anmodet ITU i 2001 om å koordinere konferanser for *World Summit on the Information Society (WSIS)*. Den første konferansen fant sted i Genève i 2003 og den andre i Tunis i 2005. På Tunis-konferansen ble blant annet følgende målsettinger vedtatt:

«We affirm that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.»

(Artikkel 42)

«We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on «Combating the criminal misuse of information technologies» and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime.»

(Artikkel 40)

WSIS anmodet ITU om å koordinere tiltak for cybersecurity innenfor rammen av WSIS Action Line C5: «Building confidence and security in the use of ICTs». ITU påtok seg oppgaven med å bygge opp tillit og sikkerhet i den globale informasjons- og kommunikasjons teknologi. ITUs generalsekretær Dr. Hamadoun I. Touré lanserte i mai 2007 *The Global Cybersecurity Agenda (GCA)* som en ramme for globale tiltak for cybersikkerhet og i kampen mot cyberkriminalitet. GCA omfatter fem hovedområder (Work Area (WA)) og den globale ekspertgruppen, HLEG, ble gitt utredningsoppdraget:

- Legal Measures (WA1)
- Technical and Procedural Measures (WA2)
- Organizational Structures (WA3)
- Capacity Building (WA4)
- International Cooperation (WA5)

The Chairman's Report

Selv om det ikke var mulig å oppnå enighet om alle anbefalinger under drøftelsene i den globale ekspertgruppen, HLEG, var det bred enighet om mange av forslagene. Det var imidlertid full enighet om viktigheten av å fremme global cybersikkerhet, og at ITU måtte ha en vesentlig rolle i dette arbeidet. Omtalen av lederens rapport *(Chairman's Report)* begrenses i denne artikkel til anbefalingene fra arbeidsgruppen WA1 som behandlet Legal Measures. (Se fakta-notis s. 35.)

Det foregår for tiden en global harmonisering av nasjonale straffe- og straffeprosessuelle lovtiltak som angår cyberkriminalitet på grunnlag av Europarådets konvensjon om cybercrime. Konvensjonen er ratifisert av 23 stater. I tillegg har 23 andre stater undertegnet konvensjonen uten ratifikasjon (januar 2009). Norge har endret bestemmelsene i straffeloven § 12, § 145, og § 145b og straffeprosessloven § 199a og § 215a for at konvensjonen kunne ratifiseres den 4. november 2005.

Med Europarådets konvensjon om cybercrime som forpliktelse, retningslinje eller referanse skapes derfor nå forutsetninger for en global rettshåndhevelse basert på felles prinsipper for straffbarhet og straffeforfølgning. Ved å ratifisere eller slutte seg til konvensjonen, eller implementere de standarder og prinsipper som den inneholder, forsikrer statene seg om at de implementeres i nasjonal lovgivning. Et effektivt internasjonalt samarbeid er avgjørende for etterforskning og straffeforfølgning av den globale cyberkriminalitet. Det viktig er at Norge og de andre land i Norden tilpasser seg sine internasjonale forpliktelser.

Lovtiltak må også gjennomføres i overensstemmelse med standarder og prinsipper i Europarådets konvensjon om forebyggelse av terrorisme av 2005. I tillegg kan den teknologiske utvikling siden cybercrimekonvensjonen ble vedtatt i 2001 medføre ytterligere lovtiltak, som for eksempel for:

Spam, identity theft, criminalization of preparatory acts prior to attempted acts, and massive and coordinated cyber attacks against the operation of critical information infrastructure.

Protokoll om cybersecurity og cyberkriminalitet

Det må reises spørsmål om nødvendigheten av å etablere nok en overordnet internasjonal avtale om lovtiltak for cyberkriminalitet. Selv om konvensjonen er akseptert av mange land også utenfor Europa, fremgår det av drøftelsene i den globale ekspertgruppen, HLEG, og av anbefalingene, at for flesteparten av andre globale regioner er og blir dette en europeisk konvensjon. Det er med andre ord behov for en legitimasjon av de aksepterte standarder og prinsipper i konvensjonen med enkelte viktige unntak i et globalt rammeverk.

Når det gjelder unntak er det nok å vise til at Russland overhodet ikke vil undertegne konvensjonen, særlig på grunn av artikkel 32 (trans-border access to stored computer data with consent or where publicly available). Mange medlemmer av den globale ekspertgruppen, HLEG, fant det nødvendig i anbefalingene å presisere at konvensjonen bare var et eksempel på et regionalt initiativ, og dette ble derfor medtatt. Det var også ønskelig å presisere at for mange land var det tilstrekkelig å anbefale konvensjonen som en referanse og intet mer. Det var en forutsetning at en implementering av konvensjonens standarder og prinsipper også var i overensstemmelse med disse lands straffelovgivning. Her var det stor variasjon i de konkrete begrunnelser.

En protokoll kan omfatte alle de fem hovedområder (WA), men er i denne artikkel begrenset til å omfatte lovtiltak i straffe- og straffeprosesslovgivningen. En første versjon som bygger på *HLEG Chairman's Report,* kan da bli som følger:

Chapter 1: Legal Measures
Article 1
Measures in Substantive Criminal Law

Considering the Council of Europe's Convention on Cybercrime as an example of legal measures realized as a regional initiative, countries should complete its ratification, or consider the possibility of acceding to the Convention of Cybercrime. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. It is very important to implement at least Articles 2-9 in the substantive criminal law section.

Countries should especially consider legislation measures against spam, identity theft, criminalization of preparatory acts prior to attempted acts, and massive and coordinated cyber attacks against the operation of critical information infrastructure.

Extending the application of existing provisions may cover criminal activities related to online games. Otherwise, countries should consider an appropriate approach to cover such offences, including a new legal framework for activities in virtual worlds.

Konvensjonens artikler om straffbare handlinger er alminnelig akseptert i de fleste land, bortsett fra artikkel 10 om vern av opphavsrettigheter og nærstående rettigheter (offences related to infringements of copyright and related rights). Mange land, særlig land i Asia har ikke slike opphavsrettlige tradisjoner som gjør det naturlig å inkludere prinsippet i en global anbefaling av tiltak. Det samme kan være tilfelle med artikkel 9 om barnepornografi (offences related to child pornography). Bestemmelser om barnepornografi har i tillegg også hjemmel i FNs barnekonvensjon. Etter mange eksperters oppfatning bør ikke slike handlinger anses som cyberkriminalitet, men etter drøftelsene i HLEG bør handlingene likevel medtas i en global anbefaling.

Ny teknologisk utvikling etter 2001 må gis særlig oppmerksomhet. Det gjelder først og fremst spam, identitetskrenkelse og phishing, men også botnets og massive, organiserte angrep på staters informasjonsinfrastruktur slik som i Estland i 2007. Flere land har vedtatt særskilte straffebestemmelse, det gjelder særlig identitetskrenkelse. I tillegg er grenseoppgangen mot terrorhandlinger allerede uklar i cyberspace.

Utviklingen av den virtuelle verden, som for eksempel *Second Life* må også følges nøye. Det kan oppstå nye behov for beskyttelse og strafferettslig vern av virtuelle interesser for en «avatar». Som dommer har jeg faktisk allerede merket meg tilbud om virtuell megling og voldgift i tilfeller hvor en «avatar» har en virtuell konflikt med en annen «avatar». Men foreløpig synes eksisterende straffebestemmelser å ramme handlinger i den virtuelle verden rimelig tilfredstillende.

Article 2
Measures in prosedural law: Investigation and Prosecution

Countries should establish the procedural tools necessary to investigate and prosecute cybercrime, as described in the Convention on Cybercrime Articles 14-22 in the section on procedural law.

The implementation of a data retention approach is one approach to avoid the difficulties of getting access to traffic data before they are deleted, and countries should carefully consider adopting such procedural legislation.

Voice over Internet Protocols (VoIP) and other new technologies may be a challenge for law enforcement in the future. It is important that law enforcement, government, the VoIP industry and ICT community consider ways to work together to ensure that law enforcement has the tools it needs to protect the public from criminal activity.

Given the ever-changing nature of ICTs, it is challenging for law enforcement in most parts of the world to keep up with criminals in their constant efforts to exploit technology for personal and illegal gains. With this in mind, it is critical that the police work closely with government and other elements of the criminal justice system, Interpol and other international organizations, the public at large, the private sector and non-governmental organizations to ensure the most comprehensive approach to addressing the problem.

International coordination and cooperation are necessary in prosecuting cybercrime and require innovation by international organizations and governments. The Convention on Cybercrime Articles 23-25 address basic requirements for international cooperation in cybercrime cases.

Prinsippene i konvensjonens straffeprosessuelle bestemmelser i artiklene 14-25 er alminnelig akseptert i mange land som nødvendige tiltak for en effektiv etterforsking og straffeforfølgning i cyberspace, både nasjonalt og i et globalt perspektiv. Enkelte land har likevel benyttet reservasjonsretten.

Kommunikasjonskontroll, avlytting av innholdsdata, pliktig datalagring i inntil to år, EUs datalagringsdirektiv 2006/24/EF, bruk av key loggers o.l. er enkelte spørsmål som har blitt særlig aktuelle etter 2001. Lovtiltak må veies mot personverninteresser i stadig større omfang. Et spesielt problem har oppstått etter innføring av Internett-telefoni (Voice over Internet Protocol, VoIP). Den gamle verbale telefonavlytting er ikke lenger mulig, og det er helt nødvendig at politi og påtalemyndighet oppdateres med hensyn til kompetanse og utstyr for å kunne etterforske straffbare handlinger.

Article 3
Measures against Terrorist misuse/use of Internet

In the fight against terrorist misuse of the Internet and related ICTs, countries should complete their ratification of the Convention on the Prevention of Terrorism of 2005. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. Article 5 on public provocation to commit a terrorist offence, Article 6 on recruitment for terrorism, and Article 7 on training for terrorism are especially important. In addition, the Convention on Cybercrime has been found to be important for defense against terrorist misuse of the Internet.

Terroristers bruk av Internett har nødvendiggjort en særskilt konvensjon med lovtiltak for å forebygge terroristhandlinger. Dette er bestemmelser som kommer til anvendelse uansett om en faktisk terrorhandling har funnet sted eller planlegges. Det er selvstendige straffbestemmelser som rammer forberedelseshandlinger, uansett om gjerningsmannen var klar over at en terrorhandling skulle finne sted eller ikke.

Hensynene til grunn for artiklene 5-7 burde også kunne anvendes i andre tilfeller av forberedelseshandlinger, f.eks. i forbindelse med forberedelser av massive, koordinerte angrep på staters informasjonsinfrastruktur i tilfeller hvor det ikke finnes bevis for forsett med hensyn til terrorhandlinger.

Article 4
Measures for the Global cooperation and exchange of information

A global conference on cybersecurity and cybercrime should be organized with the participation of regional and international organizations, together with relevant private companies. Participating organizations includes, but are not limited to: ITU, INTERPOL, United Nations Office on Drugs and Crime (UNODC), G 8 Group of States, Council of Europe, Organization of American States (OAS), Asia Pacific Economic Cooperation (APEC), The Arab League, The African Union, The Organization for Economic Cooperation and Development (OECD), The Commonwealth, European Union, Association of South East Asian Nations (ASEAN), NATO and the Shanghai Cooperation Organization (SCO).

Regionale organisasjoner har hittil ikke hatt tilbud om en konferanse med deltagelse begrenset til disse organisasjoner. Det må antas at de regionale organisasjoner har behov for en gjensidig dialog om mange administrative og organisasjonsmessige spørsmål. Formålet med en slik konferanse om cybersikkerhet og cyberkriminalitet er å utveksle informasjon med sikte på å oppnå eller koordinere felles intensjoner for prinsipper og standarder for en global bekjempelse av cyberkriminalitet. Dette må også inkludere massive og koordinerte angrep på statenes informasjonsstruktur, og terroristers bruk av Internett. Konferansen vil fremme sikkerhet i cyberspace, og må inkludere anbefaling av lovtiltak som er globalt akseptert. Strategien for en løsning vil være å forene eksisterende regionale initiativer, med sikte på anbefalinger som kan aksepteres av alle regionale organisasjoner. En slik konferanse planlegges for tiden, og kan bli en realitet allerede i løpet av 2009.

Article 5
Measures on Privacy and Human Rights

In conducting cybercrime investigation and prosecution, countries should ensure that their procedural elements include measures that preserve the fundamental rights to privacy and human rights, consistent with their obligations under international human rights law. Preventive measures, investigation, prosecution and trial must be based on the rule of law, and be under judicial control.

De tiltak som iverksettes må respektere internasjonale rettsikkerhets-

instrumenter i FN-konvensjoner, som alle stater er bundet av. Tiltakene må være basert på rettsikkerhetsgarantier underlagt judisiell eller annen rettslig kontroll.

Stein Schjølberg er sorenskriver Moss tingrett.

Lov&Data gratulerer

© ITU/V. Martin

På ITUs rådsmøte i november 2008 ble Stein Schjølberg tildelt ITUs sølvmedalje av generalsekretær Dr. Hamadoun I. Touré for som en anerkjennelse av hans betydningsfulle bidrag til ITUs arbeid ang. cybersikkerhet og cyberkriminalitet. Schjølberg er en internasjonal ekspert når det gjelder cyberkriminalitet, og han er en av grunnleggerne når det gjelder arbeidet med å harmonisere nasjonal lovgivning i forhold til cyberkriminalitet. *Lov&Data* gratulerer!

(Kilde: *http://www.itu.int/osg/csd/cybersecurity/gca/hleg/silvermedal.html)*

Fakta-notis: Anbefalinger fra arbeidsgruppen WA1 (legal measures)

Den fullstendige Chairman's Report med de øvrige fire hovedområder (WA2-WA5) er tilgjengelig på *http://www.itu.int/osg/csd/cybersecurity/gca* og *http://www.cybercrimelaw.net*. Kommentater fra enkelte av de over 100 HLEG medlemmer under den avsluttende debatten finnes i kursiv under hvert punkt.

Overview
Work Area one (WA1) sought to promote cooperation and provide strategic advice to the ITU Secretary-General on legislative responses to address evolving legal issues in cybersecurity. Some HLEG members considered that the scope of WA1 included prosecution of cybercrimes. One member suggested the following summary of WA1: «ITU's Secretary-General should promote cooperation among the different actors so that effective legal instruments are identified and characterized in building confidence and security in the use of ICTs, making effective use of ITU recommendations and other standards, in accordance with present international agreements».

Summary of Discussions
Discussions covered how to build on existing agreements in this area: for example, the Council of Europe's Convention on Cybercrime and the Convention on the Prevention of Terrorism of 2005. Some members preferred omitting mention of the Convention on Cybercrime, although they recognized it as an available reference. One member stated that the Convention on Cybercrime could not be proposed as the only solution for all states and wished to acknowledge the status of the Convention as an example of legal measures realized as a regional initiative belonging to signatory countries, consistent with the status accorded to the Convention in paragraph 40 of the WSIS Tunis Agenda for the Information Society.

There was considerable discussion as to whether recommendations 1.1-1.3 should be merged. Some members supported the suggestion that Recommendations 1.1-1.3 should be merged (e.g. some members wished to delete Recommendation 1.3). One key recommendation emerging from WA1 was that ITU could organize a global conference to promote cybersecurity, but this was contentious for some HLEG members (recommendation 1.13).

WA1 Recommendations
1.1. ITU is a leading organisation of the UN system and could elaborate strategies for the development of model cybercrime legislation as guidelines that are globally applicable and interoperable with existing national and regional legislative measures.

1.2. Governments should cooperate with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks: for example, UNGA Resolutions 55/63 and 56/121 on «Combating the criminal misuse of information technologies» and regional relevant initiatives including, but not limited to, the Council of Europe's *Convention on Cybercrime*.

1.3. Considering the Council of Europe's Convention on Cybercrime as an example of legal measures realized as a regional initiative, countries should complete its ratification, or consider the possibility of acceding to the Convention of Cybercrime. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice.

With regard to the Council of Europe's Convention on Cybercrime, some members suggested that countries could be encouraged to join and ratify the Convention and draw on it in drafting their relevant legislation. One member suggested that countries could, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. Other members preferred omitting mention of the Convention on Cybercrime, although they recognized it as an available reference, whilst one member stated that the Convention could not be proposed as the only solution for all states and wished to acknowledge that the Convention is an example of legal measures realized as a regional initiative belonging to those countries which are signatories, consistent with the status accorded to the Convention in paragraph 40 of the WSIS Tunis Agenda for the Information Society. Some members wished to delete recommendation 1.3, despite the insertion of text recognizing the Convention as a regional initiative. One member wished to delete the phrase «may want to» in recommendation 1.3.

1.4. It is very important to implement at least Articles 2-9 in the substantive criminal law section, and to establish the procedural tools necessary to investigate and prosecute such crimes as described in Articles 14-22 in the section on procedural law.

A few members wished to delete this recommendation.

1.5. Cybercrime legislation should be designed using existing international and regional frameworks as a reference or as a guideline, and the Convention on Cybercrime was designed in a way so that it could be adapted to technological developments, and laws using the Convention as a guideline should be able to address modern developments.

One member wished to delete the first phrase on how cybercrime legislation should be developed. A few other members wished to delete the text referring to the history of the design of the Convention and the normative statement as to what it might be able to achieve.

1.6. Discussions about how to address criminal activities related to online games have just begun. Currently, most states seem to focus on extending the application of existing provisions, instead of developing a new legal framework for activities in virtual worlds. Depending on the status of cybercrime-related legislation, most offences should be covered this way; otherwise, countries should consider an appropriate approach to cover such offences.

One member wished to delete this Recommendation.

1.7. Supplementing Articles in the Convention may however be necessary. Countries should especially consider legislation efforts against spam, identity theft, criminalization of preparatory acts prior to attempted acts, and massive and coordinated cyber attacks against the operation of critical information infrastructure.

A few members wished to delete the first sentence referring to the need for supplementing Articles in the Convention.

1.8. Countries should consider how to address data espionage and steps to prevent pornography being made available to minors.

One member considered that the term «data espionage» is ambiguous, and should be defined properly, whilst another member wished to remove this term. Two members wished to delete this recommendation.

1.9. The introduction of new technologies always presents an initial challenge for law enforcement. For example, VoIP and other new technologies may be a challenge for law enforcement in the future. It is important that law enforcement, government, the VoIP industry and ICT community consider ways to work together to ensure that law enforcement has the tools it needs to protect the public from criminal activity.

1.9.a. Given the responsibility of government authorities in protecting their consumers, special attention should be given to requirements enacted by government authorities that bear directly on the infrastructure-based and operational requirements imposed on those who provide and operate network infrastructures and services, or supply the equipment and software, or end-users. The concept of shared responsibilities and responsible partnership should be underscored in the development of legal measures on cybersecurity obligations in civil matters. A coordinated approach between all parties is necessary to develop agreements, as well as provide civil remedies in the form of judicial orders for action or monetary compensation instituted by legal systems when harm occurs.

Two members wished to delete this recommendation. Some members wished to replace the specific references to VoIP with more general text recognizing that the introduction of a broad range of new technologies presents initial challenges for law enforcement. One member supported reference to «government, industry and ICT community», whilst another wished to make more general reference to «all relevant parties» [who] «should work together to ensure that law enforcement has the tools, resources and training needed». One member proposed the specific insertion of the additional text in 1.9(a).

1.10. The implementation of a data retention approach is one approach to avoid the difficulties of getting access to traffic data before they are deleted, and countries should carefully consider adopting such procedural legislation.

Two members wished to delete this recommendation. Another member proposed the alternative text: «the implementation of a data preservation approach has proven to be a key resource to law enforcement in investigations. Development of a balanced and reasonable data retention requirement should be carefully examined, taking into account expectations of privacy, security risks, etc., when considering adopting such procedural legislation».

1.11. In the fight against terrorist misuse of the Internet and related ICTs, countries should complete their ratification of the *Convention on the Prevention of Terrorism of 2005*. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. Article 5 on public provocation to commit a terrorist offence, Article 6 on recruitment for terrorism, and Article 7 on training for terrorism are especially important. In addition, the *Convention on Cybercrime* has been studied with relation to terrorist misuse of the Internet and has been found to be important for defense against it.

One member wished to delete the last sentence.

1.12. Given the ever-changing nature of ICTs, it is challenging for law enforcement in most parts of the world to keep up with criminals in their constant efforts to exploit technology for personal and illegal gains. With this in mind, it is critical that police work closely with government and other elements of the criminal justice system, Interpol and other international organizations, the public at large, the private sector and non-governmental organizations to ensure the most comprehensive approach to addressing the problem.

General consensus was achieved in respect of this recommendation.

1.13. There are several challenges facing prosecutors today in order to successfully prosecute cybercrime cases. These challenges include: 1) implementation of relevant cybercrime legislation; 2) understanding the technical evidence; 3) collecting evidence abroad; and 4) being able to extradite suspects located abroad. Thus, international coordination and cooperation are necessary in prosecuting cybercrime and require innovation by international organizations and governments, in order to meet this serious challenge. The *Convention on Cybercrime* Articles 23-25 address basic requirements for international cooperation in cybercrime cases.

One member wished to delete the last sentence, while several other members wished to extend the reference to the Articles mentioned, with the replacement of Article 25 with 35.

1.14. In conducting cybercrime investigation and prosecution, countries should ensure that their procedural elements include measures that preserve the fundamental rights to privacy and human rights, consistent with their obligations under international human rights law. Preventive measures, investigation, prosecution and trial must be based on the rule of law, and be under judicial control.

General consensus was achieved in respect of this recommendation.

1.15. The ITU, as the sole Facilitator for WSIS Action Line C5, should organize a global conference with the participation of [ITU Membership] for Members, regional and [international] organizations on cybersecurity and [relevant private organizations] in cybercrime. Participating organizations include, but are not limited to: INTERPOL, United Nations Office on Drugs and Crime (UNODC), G 8 Group of States, Council of Europe, Organization of American States (OAS), Asia Pacific Economic Cooperation (APEC), The Arab League, The African Union, The Organization for Economic Cooperation and Development (OECD), The Commonwealth, European Union, Association of South East Asian Nations (ASEAN), NATO and the Shanghai Cooperation Organization (SCO).

Many members supported the recommendation of a global conference to promote cybersecurity, whilst other members wished to remove this recommendation – one member voiced its strong opposition to this. One member emphasized that ITU conferences should be open in its membership, especially to developing countries, whilst another underlined the importance of ITU remaining open to collaboration. Several members included reference to ITU's mandate as Facilitator for WSIS Action Line C5 and proposed insertions in square brackets refining the scope of the stakeholders involved.