Stein Schjolberg

Terrorism in Cyberspace – Myth or reality?

"Those who fail to anticipate the future are in for a rude shock when it arrives"
Professor Peter Grabosky, Australia

All countries are struggling to adapt their criminal justice systems to the threat posed by terrorism. However, combating terrorism is fundamental in order to guarantee the security and freedom of all citizens. However, the fight against terrorism should not be seen as a "war". Terrorism must be regarded as a crime, albeit a particularly serious one, and should be commanded as such. Preventive measures, investigation, prosecution and trial must be founded on the rule of law, be under judicial control and based on the international recognized human rights principles as enshrined in the United Nations Human Rights Conventions and the European Convention on Human Rights.

Those were the words of Attorney Generals or General Prosecutors from 30 European States in a statement at the Ninth Annual Eurojustice Conference in September 2006.[1]

Terrorism has been used to describe criminal conducts long before the computer communication and network technology was introduced. International organizations have been involved in the prevention of such acts for a long period, but the global society has not yet been able to agree upon a universal definition on terrorism. In the final conference on preparing for the establishment of an international criminal court,[2] other serious crimes such as terrorism were discussed, but the conference regretted that no generally acceptable definition could be agreed upon.

Chief Judge Stein Schjolberg is an international expert on cybercrime and one of the founders of the global harmonization of national criminal law on computer crime, see www.cybercrimelaw.net/content/about.html
This paper is based on presentations by the author at the NATO Advanced Research Workshop on Cyberterrorism, Sofia, Bulgaria (October 2006), and at the International Criminal Law Network (ICLN) 4th Annual Conference: Effective Counter-Terrorism and the Rule of International Law, The Hague, The Netherlands (December 2005). steins@mosstingrett.no www.cybercrimelaw.net www.globalcourt.com

[1] www.eurojustice.org

[2] Final Act of the United Nations diplomatic conference of plenipotentiaries on the establishment of an International Criminal Court, Rome July 17, 1998 (U.N. Doc. A/CONF.183/10).

Expert Papers on Cybercrime No. 1/2007 © Stein Schjølberg 2007

The *Expert Papers on Cybercrime* series are comments on enforcement and legal issues by world leading experts in the field. The series is published by CybercrimeData. Experts are invited to publish their papers on this web site.

In Europe a Council of Europe treaty "The European Convention on the Suppression of Terrorism" was adopted in 1977 as a multilateral treaty. The treaty was in 2005 supplemented by the Council of Europe Convention on the Prevention of Terrorism.[3] In this convention a terrorist offence is merely defined as meaning any of the offences as defined in the attached list of 10 treaties in the Appendix. But the purpose or intent of a terrorism offence is described in the convention as:

> by their nature or context to seriously intimidate a population or unduly compel a government or an international organization to perform or abstain from performing any act or seriously destabilize or destroy the fundamental political, constitutional, economic or social structures of a country or an international organization.

Terrorism in cyberspace consists of both cybercrime and terrorism. Terrorist attacks in cyberspace are a category of cybercrime and a criminal misuse of information technologies.[4] The term "cyberterrorism" is often used to describe this phenomenon.[5] But while using such term, it is essential to understand that this is not a new category of crime.

Cyberterrorism has been defined as unlawful attacks and threats of attack against computers, networks, and stored information. It has to intimidate or coerce a government or its people in furtherance of political or social objectives. An attack should result in violence against persons or property, or at least cause enough harm to generate fear. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact.[6]

Another definition covers a criminal act perpetrated by the use of computers and telecommunications capabilities causing violence, destruction and/or disruption of services. The purpose must be to create fear by causing confusion and uncertainty in a population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda.[7]

Cyberterrorism has also been defined as attacks or series of attacks on critical information infrastructures carried out by terrorists, and instills fear by effects that are destructive or disruptive, and has a political, religious, or ideological motivation.[8]

These definitions have one thing in common, the conducts must be acts designed to spread public fear, and must be made by terrorist intent or motivation. Terrorism in cyberspace includes the use of information technology sys-

---

[3] The Council of Europe Convention on the Prevention of Terrorism will enter into force June 1, 2007.
[4] See ASEAN Regional Forum Statement on cooperation in fighting cyber attack and terrorist misuse of cyberspace (June 2006).
[5] John Malcolm, Deputy Assistant Attorney General, US Department of Justice: Virtual Threat, Real Terror: Cyberterrorism in the 21st Century; Testimony before the US Senate Committee on the Judiciary, February 24, 2004.
[6] Dorothy E. Denning, Professor, Naval Postgraduate School, USA: Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 2000.
[7] Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI: Terrorism, Technology, and Homeland Security. Testimony before the Senate Judiciary Subcommittee, February 24, 2004.
[8] See the International Handbook on Critical Information Infrastructure Protection (CIIP) 2006 Vol. II, page 14.

tems that is designed or intended to destroy or seriously disrupt critical information infrastructure of vital importance to the society and that these elements also are the targets of the attack.[9]

This paper is aimed at presenting some issues of terrorism in cyberspace, including the international legal coordination and recommendations, and the rule of law.

Conducts of terrorism in cyberspace

The potential threats of attacks by terrorists in cyberspace would focus on systems and networks that contains critical information infrastructure. It may include conducts against the confidentiality, integrity and availability of such systems and networks through cybercrimes: illegal access, illegal interception, data interference, system interference, and misuse of devices.[10]

Serious hindering of the functioning of a computer systems and networks of the critical information infrastructure of a State or government would be the most likely targets. The dependency of information and communication technology creates at the same time a vulnerability that is a challenge for cyber security. Attacks against critical information infrastructures may cause comprehensive disturbance and represent a significant threat that may have the most serious consequences to the society.

Potential targets may be governmental systems and networks, telecommunications networks, navigation systems for shipping and air traffic, water control systems, energy systems, and financial systems, or other functions of vital importance to the society. It should constitute a criminal offence when terrorists are able of hindering or interrupting the proper functioning, or influence the activity of the computer system, or making the system inoperative e.g. crashing the system. Computer systems can thus be closed down for a short or extended period of time, or the system may also process computer data at a slower speed, or run out of memory, or process incorrectly, or to omit correct processing. It does not matter if the hindering being temporarily or permanent, or partial or total.

Hindering or interruption may be caused by a Denial-of-Service (DOS) attack.[11] The most potential denial of service attacks by terrorists in cyberspace is flooding computer systems and networks with millions of messages from networks of hundreds of thousands of computers from all over the world in a coordinated cyberattack. Such an attack has a potential to crash or disrupt a significant part of a national information infrastructure and may be caused by botnets.[12]

---

[9] See also Kathryn Kerr, Australia: Putting cyberterrorism into context. (2003)

[10] See Council of Europe Convention on Cybercrime, Articles 2-6.

[11] A Denial-of-Service attack (DoS attack) is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system (see Wikipedia).

[12] Botnet is a jargon term for a collection of software robots, or bots, which run autonomously (see Wikipedia). In criminal offences they can be secretly installed on a target computer system for later use by an unau-

Categories of such attacks are also blocking users from legitimate access by entering wrong passwords for correct user name in order to block the access for that user name. Or triggering a denial of service attack alert without the existence of any such attack at all, so that the computer system really restricts access to anyone.

Terrorist offences in cyberspace and attacks on critical information infrastructures are cybercrimes.

Massive and coordinated cyber attacks were in May 2007 launched against websites of the government, banks, telecommunications companies, Internet service providers and news organizations in Estonia. The attacks have been described as targeted and well organized from outside Estonia, and were attacks on the public and private critical information infrastructure of a State. It was estimated that 1 million computers around the world were involved through the use of botnets. Some described it as "the Big Bang" as 4 million packets of data per second, every second for 24 hours, bombarded a host of targets that day. The attacks forced banks to shut down online services for all customers for an hour and a half, and disrupted government communications.[13]

The purposes and intent of the attacks may be described as terrorist purposes included in the Council of Europe Convention on the Prevention of Terrorism of 2005, if they fulfill the requirement of: *"…seriously destabilize or destroy the fundamental political, constitutional, economic or social structure of a country…"*

Preparatory criminal conducts

It is assumed that terrorists so far are using cyberspace as a tool for organizing, exchange of information, recruiting and fundraising. Websites may also be used for training and propaganda.

According to the 2005 Council of Europe Convention on the Prevention of Terrorism, Articles 5-7, parties to the Convention are required to adopt certain preparatory conducts that have a potential to lead to terrorist acts as criminal offences.[14]

Public provocation to commit a terrorist offence is a criminal offence if the distribution of a message to the public, "whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed" (Article 5). Presenting a terrorist offence as necessary and justified is a criminal offence.[15] A specific intent is required *to incite the commission of a terrorist offence.* The provocation must in addition be committed unlawfully and intentionally.

Recruitment for terrorism is also a criminal offence if a person is solicited "to commit or participate in a commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one

thorized remote user, when taking control of the system and giving out malicious directions for a group of other bots and launch a denial of service attacks in coordinated cyber attacks.

[13] See www.washingtonpost.com

[14] See http://conventions.coe.int

[15] See Explanatory Report note 98.

or more terrorist offences by the association or the group" (Article 6). The recruitment for terrorism may be carried out through the use of Internet, but it is required that the recruiter successfully approach the person. The recruitment must be unlawfully and intentionally.

Training for terrorism is a criminal offence if instructions are provided for "making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques" (Article 7). The purpose must be to execute the terrorist offence or contribute to it. The trainer must have knowledge of that skills or "know-how" and intended to be used for the carrying out of the terrorist offence or for a contribution to it.[16] The training must be unlawfully and intentionally.

Public provocation, recruitment or training for a coordinated cyber attack with terrorist intent to destroy or seriously disrupt information technology systems or networks of vital importance to the society may constitute as a criminal offence.

In one of the first convictions of this category, a man was on April 11, 2007, sentenced in København Byret (Copenhagen District Court)[17] in Denmark, to imprisonment for 3 year and 6 months for a violation of Danish Penal Code. He had encouraged to terrorist acts by collecting materials of previous terrorists' acts and other terrorists material. His acts were not even connected to any specific terrorist acts. The court stated also as follows:

> The defendants activity may be described as professional general advices to terrorist groups that are intended to commit terrorist acts and that the defendant knew that, including that the spreading of his materials were suitable for recruiting new members to the groups, and suitable for the members of the groups to be strengthened in their intent to commit terrorist acts.

International Legal Assistance

The Attorney Generals Conference

The Ninth Annual Eurojustice Conference[18] was held in Oslo, September 27-29, 2006. Attorney Generals or General Prosecutors from 30 States discussed various aspects of the challenge of terrorism and the fight against this crime.

The conference stressed the importance of cooperation and coordination in the fight against terrorism and pointed out that all authorities and institutions of a society have a vital role in this fight. A success can only be obtained by cooperation and exchange of information, and efforts from the society as a whole. The conference stated that acts of terrorism may take place anywhere in the world and the response must be global with cross border cooperation.

The conference especially emphasized that there is no war against terrorism, other than a regular fight against a serious crime. The combat must be founded on the rule of law under judicial control, and based on principles recognized by

[16] See Explanatory Report note 122.
[17] See www.domstol.dk/KobenhavnsByret
[18] See www.eurojustice.org

international Human Rights Conventions. Threats of or use of torture, or use of evidence stemming from threats or torture, must never be accepted.

The Hague Conference on Effective Counter-Terrorism and the Rule of International Law

A conference on effective counter-terrorism and the rule of international law was held in The Hague in December 2005. The conference was organized by the International Criminal Law Network (ICLN), which is also based in The Hague, and focused on the balance between counter-terrorism measures and the rule of law.

At the session on cyberterrorism it was emphasized that no single instance of real terrorism in cyberspace was publicly known. The discussion demonstrated that terrorism in cyberspace was not yet a realistic threat, but the speakers agreed on a potential threat. The real threat in terms of terrorism in cyberspace is coming more from the massive usage of cyberspace as propaganda, education and fundraising tool, and as such the web is the strongest weapon of the terrorist organization.[19]

International mutual legal assistance in investigation and prosecution of terrorism in cyberspace

Where formal assistance is needed, evidences must be collected in such a way that the requesting State could admit the information into the domestic court.

The Council of Europe Convention on Cybercrime[20] provides in Chapter III on International cooperation (Articles 23-35), an extensive review of the types and conditions of formal mutual legal assistance efforts needed between countries to trace criminals through cyberspace. They include a 24/7 network, extradition, general principles relating to mutual assistance, spontaneous information, procedures pertaining to mutual assistance requests in the absence of applicable international agreements, confidentiality and limitation on use, mutual assistance on expedited preservation of stored computer data and on expedited disclosure of preserved traffic data, mutual assistance regarding investigative powers on accessing of stored computer data and in the real-time collection of traffic data and interception of content data, and transborder access to stored computer data with consent or where publicly available.

Without ratification or acceding to the Council of Europe Convention, States will rely on multilateral or bilateral legal instruments that outline the procedures each State must follow. Without any such legal instruments, States must rely on traditional means including formal requests for assistance between government and official authorities. Where compatible substantive and procedural laws exist, mutual legal assistance often naturally develops building on mechanisms that already exist for traditional crimes. It is important to observe

[19] Katharina von Knop: The soft Power of the electronic Jihad, ICLN Annual Conference: Effective Counter-Terrorism and the Rule of International Law (2005), The Hague, The Netherlands.
[20] See www.coe.int

the principles of "extradite or prosecute", avoiding "safe havens" for terrorists in cyberspace.

Interpol offers rapid response capabilities, including the global police communications system, the I-24/7. This real-time, operational support for police work worldwide, via the Command and Co-ordination Centre at the General Secretariat in Lyon, France, operates 24 hours a day, 7 days a week. In addition, regional support structures and national structures, including the implementation of operations or targeted projects on priority or specific types of crime and notice system designed to warn police departments about wanted persons, which also comes within the context of cooperation with other international bodies.

The G 8 Group 24/7 network consists of almost forty countries worldwide.[21] These countries provide points of contact available around-the-clock, trained in computer investigations and able to initiate the administrative procedures necessary to preserve and acquire computer evidence.

The Rule of Law in Criminal Courts of Justices

The Role of the Court of Justices

The national Court of Justices is the main legal guarantee on promoting the national rule of law on terrorist acts in cyberspace. The role of judges in protecting the rule of law and human rights in the context of terrorism in cyberspace has the same framework as in all categories of terrorism. The Consultative Council of European Judges (CCJD) has adopted in 2006 the following principles:[22]

> While terrorism creates a special situation justifying temporary and specific measures that limit certain rights because of the exceptional danger it poses, these measures must be determined by the law, be necessary and be proportionate to the aims of a democratic society.
>
> Terrorism cases should not be referred to special courts or heard under conditions that infringe individuals right to a fair trial.
>
> The courts should, at all stages of investigations, ensure that restrictions of individual rights are limited to those strictly necessary for the protection of the interests of society, reject evidence obtained under torture or through inhuman or degrading treatment and be able to refuse other evidence obtained illegally.
>
> Detention measures must be provided for by law and be subject to judicial supervision, and judges should declare unlawful any detention measure that are secret, unlimited in duration or do not involve appearance before established according to the law, and make sure that those detained are not subjected to torture or other inhuman or degrading treatment.

[21] Australia, Austria, Brazil, Canada, Croatia, Denmark, the Dominican Republic, Finland, France, Germany, Hungary, India, Indonesia, Israel, Italy, Japan, Republic of Korea, Luxembourg, Malaysia, Mexico, Morocco, the Netherlands, New Zealand, Norway, Philippines, Romania, Russia, Singapore, South Africa, Spain, Sweden, Thailand, Tunisia, the United Kingdom, the United States, and the territories of Hong Kong and Taiwan. (March 2007).

[22] Adopted November 11, 2006 by the Consultative Council of European Judges (CCJE), a Council of Europe advisory body.

> Judges must also ensure that a balance is struck between the need to protect the witnesses and victims of acts of terrorism and the rights of those charged with the relevant offences.
>
> While States may take administrative measures to prevent acts of terrorism, a balance must be struck between the obligation to protect people against terrorist acts and the obligation to safeguard human rights, in particular through effective access to judicial review of the administrative measures.

Any Government has a responsibility to protect the people. The political branches of government formulate and implement the means adopted to protect citizens against the threat of terrorism. They may do so only by lawful means, but the ultimate responsibility of deciding issues of lawfulness rests with the judicial courts.[23]

Two very important cases should be emphasized. In United Kingdom, the House of Lords unanimously held in a decision that if it appeared that evidence had been obtained through torture, it could not be used against terror suspects in British courts.[24] Lord Bingham of Cornhill, the Head of the panel, stated:

> The principles of the common law, standing alone, in my opinion compel the exclusion of third party torture evidence as unreliable, unfair, offensive to ordinary standards of humanity and decency and incompatible with principles, which should animate a tribunal seeking to administer justice.

An even more famous decision, the US Supreme Court held that military commission proposed to try prisoners in Guantanamo Bay was not a legal body. The military commission was a tribunal not mentioned in the US Constitution or created by existing statutes. The Court held that neither of the congressional Acts expands the President's authority to convene military commissions, and it contains no language authorizing that tribunal at Guantanamo Bay. The Supreme Court further held that the procedures adopted also violated the Geneva Conventions, and at least Common Article 3 applied in the case. According to the Article, Each Party shall be bound to apply certain provisions, and the Court further stated:

> One such provision prohibits "the passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court affording all the judicial guarantees which are recognized as indispensable by civilized peoples".[25]

The Role of the International Criminal Court

The International Criminal Court was established in 1998 by 120 States at a conference in Rome. The Rome Statute of the International Criminal Court was adopted and it entered into force on July 1st, 2002.[26]

The International Criminal Court (ICC) is the first ever permanent, treaty based, fully independent international criminal court established to promote the rule of law and ensure that the gravest international crimes do not go unpun-

---

[23] Chief Justice Murray Gleeson, Australia: A Core Value. A presentation at the Judicial Conference of Australia Annual Colloquium, Canberra October 6, 2006.
[24] Opinions of the Lords of Appeal on December 8, 2005, by a panel of seven Law Lords.
[25] See Hamdan v. Rumsfeld, Secretary of Defence, Decided June 29, 2006, page 67.
[26] See www.icc-cpi.int/about/ataglance/history.html

ished. The Court do not replace national courts, the jurisdiction is only complementary to the national criminal jurisdictions. It will investigate and prosecute if a State, party to the Rome Statute, is unwilling or unable to prosecute. Anyone, who commits any of the crimes under the Statute, will be liable for prosecution by the Court.

The jurisdiction of the International Criminal Court is limited to States that becomes Parties to the Rome Statute, but then the States are obliged to cooperate fully in the investigation and prosecution.

Article 5 limits the jurisdiction to the most serious crimes of concern to the international community as a whole. This may also be understood as an umbrella for future developments.[27] The article describes the jurisdiction including crimes of genocide, crimes against humanity, war crimes and crimes of aggression.

In the final diplomatic conference in Rome,[28] other serious crimes such as terrorism crimes were discussed, but the conference regretted that no generally acceptable definition could be agreed upon. The conference recognized that terrorist acts are serious crimes of concern to the international community, and recommended that a review conference pursuant to the article 123 of the Statute of the International Criminal Court consider such crimes with the view of their inclusion in the list within the jurisdiction of the Court.

With a reference to the Rome conference, expanding the Statute to include terrorism is recommended. The International Criminal Court should also have a role in the fight against international terrorism in cyberspace. Individual States may be unwilling or unable to exercise jurisdiction on such a case. According to article 17, unwilling is a State whenever it appears to be a lack of genuine will to investigate or prosecute the crime. A State is unable whenever it appears to be a total or substantial collapse of its judicial system, or by some reason is unable to obtain the accused or the necessary evidence and testimony or otherwise unable to carry out its proceedings due to its unavailability.

Another scenario for sending a case on terrorism in cyberspace to the International Criminal Court would be whenever a State, despite of being willing and able, waives the jurisdictional power and defers the case to the Court. In such instances the State may consider the Court to be in a better position to investigate and prosecute as the independent institution for international crimes.

The International Criminal Court may have a role to play in the fight against terrorism in cyberspace even today under the current jurisdiction in force.[29] According to article 93, paragraph 10, the Court may upon request " cooperate with and provide assistance to a State Party conducting an investigation into or trial in respect of conduct which constitutes a crime within the jurisdiction of the Court or which constitutes a serious crime under the national law of the

[27] See www.un.org/law/icc/statute/99_corr/2.htm

[28] Final Act of the United Nations diplomatic conference of plenipotentiaries on the establishment of an International Criminal Court, Rome July 17, 1998 (U.N. Doc. A/CONF.183/10).

[29] See Federica Gioia: The ICC and terrorism in the light of the principle of complementarity, ICLN Annual Conference (2005).

requesting State." Terrorism in cyberspace qualifies undoubtedly as a "serious crime".

The cyber attacks in Estonia in May 2007 may qualify as a "serious crime", and as such the International Criminal Court may upon request from a State Party conducting investigation into or trial for the case.

The Rule of Law on Terrorism in Cyberspace

A binding global legal instrument such as the Rome Statute of the International Criminal Court may strengthen the global integration of procedural and court proceedings on terrorism in cyberspace. The Rome Statute may create a global judicial framework ensuring against immunity from the appropriate sanctions of terrorist acts. It may also improve the decision-making in the global law enforcement and procedural cooperation on the basis of the current United Nations conventions and universal instruments on terrorism.

If terrorist acts are included in the jurisdiction of the International Criminal Court, the Rome Statute has Articles on investigation, prosecution and three divisions of Courts for normal and formal proceedings. But the Prosecutor, which is an independent organ of the Court, may after having evaluated the information made available, initiate investigation also on an exceptional basis. (Articles 18 and 53) In accordance with Article 18 on preliminary rulings regarding admissibility, the Prosecutor may "seek authority from the Pre-Trial Chamber to pursue necessary investigative steps for the purpose of preserving evidence where there is a unique opportunity to obtain important evidence or there is a significant risk that such evidence may not be subsequently available." Such an exceptional proceeding may very well be needed in investigations of terrorist attacks in cyberspace. It is also the Pre-Trial Chamber that later on eventually issues an arrest warrant.

The Court may exercise its functions and powers on the territory of all States Parties to the Rome Statute, and the maximum term of imprisonment is 30 years, and also a life sentence may be imposed.

The Role of International Organizations on terrorism in Cyberspace

International and regional organizations have been active in harmonizing national legislation on cybercrimes, also covering conducts terrorists may use in cyberspace. The focus should be on serious crimes against information technology.[30] Based on the international legal standards and principles in the Council of Europe Convention on Cybercrime, and the recommendations from the United Nations, G8 group, European Union, Asian Pacific Economic Cooperation (APEC), Organization of American States (OAS), The Commonwealth,

[30] Seymour E. Goodman: Toward a Treaty-Based International Regime on Cyber Crime and Terrorism.

ASEAN Group, and the OECD, we have an emerging global legal framework on cybercrime, also including terrorism.

United Nations

Various United Nations institutions have provided significant efforts on a number of cyberspace topics, including terrorism and combating the criminal misuse of information technology. The United Nations General Assembly Resolution adopted in 2000[31] addressed various ways States could strive to combat the criminal misuse of information technologies.

Various other Resolutions have been adopted, among them Resolution 57/239 in 2002 on the Creation of a global culture of cyber-security. The General Assembly adopted a new Resolution 58/199 in 2003, on the Creation of a global culture of cyber-security and the protection of critical information infrastructure. This Resolution also invited the member states to take into account the principles in the preparation for the World Summit on the Information Society (WSIS) in Tunis in 2005. Based on the 2005 World Summit Outcome Document, a global counter-terrorism strategy was adopted by the General Assembly in 2006.[32] The strategy included a statement as follows:

> Reaffirming that acts, methods and practices of terrorism in all its forms and manifestations are activities aimed at the destruction of human rights, fundamental freedoms and democracy, threatening territorial integrity, security of States and destabilizing legitimately constituted Governments, and that the international community should take the necessary steps to enhance cooperation to prevent and combat terrorism.

The Security Council's Counter-Terrorism Committee is the main committee and leading body to promote collective actions on counter-terrorism efforts in the United Nations. The committee was established by the Security Council on September 28, 2001 in Resolution 1373 (2001) and given the commissions in the Security Council's Resolution 1377 (2001) and Resolution 1535 (2004). The Security Council Resolution 1373 (2001) is a historic document that obliged States to apply a list of principles in the fight against terrorism. The resolution is one of the principal components of the international legal regime against terrorism and was adopted in the aftermath of the 9/11 attacks in New York. It declares that acts, methods and practices of terrorism are contrary to the purposes and principles of the United Nations, and calls upon member States to become parties to the relevant international conventions and protocols.

The Security Council Resolution 1624 (2005) on the fight against terrorism is similar to the Council of Europe Convention on the Prevention of Terrorism of 2005, see III.2.

---

[31] The resolution was adopted by the General Assembly on December 4, 2000 (A/res/55/63). See www.unodc.org/unodc/crime_cisp_resolutions.html

[32] The Strategy was adopted by the General Assembly on September 8, 2006 (A/res/60/288).

United Nations Office on Drugs and Crime (UNODC)

The United Nations Office on Drugs and Crime in Vienna, Austria,[33] is the organizer of the United Nations Crime Congresses and has established the Terrorism Prevention Branch.

The Crime Congress in 2005 in Bangkok, Thailand, discussed issues of computer-related crime in a special workshop, and the strengths and weaknesses of the international legal instruments on counter-terrorism in a special committee.[34] The delegates emphasized a need to make these instruments truly universal.

The United Nations have at least 12 universal instruments on terrorism and 85 States (December 2006) have ratified all of them. The UNODC Terrorism Prevention Branch provides legal advices to States on becoming parties to these universal instruments and promotes global cooperation.

International Telecommunication Union (ITU)

The most active United Nations institution in reaching harmonization on global cybersecurity and cybercrime legislation is the International Telecommunication Union (ITU) in Geneva. As a follow-up from the 2005 World Summit on the Information Society Summit (WSIS) in Tunis a consulting meeting on Partnerships for Global Cybersecurity was held at the ITU in May 2006. It was a Facilitation Meeting for WSIS Action Line C5: Building confidence and security in the use of ICT.[35]

Three focus areas were established for future capacity building.[36] The first area covers sharing information between States, especially of policies on addressing cybersecurity and critical information infrastructure protection (CIIP). Capacity building based on "a generic model framework or toolkit that national policy-makers could use to develop and implement a national cybersecurity or CIIP programme" should be established.

The second area covers harmonizing the national legal approaches and international legal coordination on cybercrime. Implementing the basic international legal standards and principles on cybercrime in national legislation is essential for a global cybersecurity. Capacity building based on "the harmonization of cybercrime legislation, and enforcement" should be established.

The third area covers developing watch, warning and incident response capabilities. Sharing information between States on such capabilities is essential for a global cybersecurity. Capacity building based on "developing watch, warning and incident response capabilities" should be established.

---

[33] See www.unodc.org

[34] The Crime Congress website is located at: http://www.unodc.org/unodc/crime_congress_11/documents.html An excellent presentation of the role of UNODC in terrorism prevention can be found on the website.

[35] See www.itu.int/cybersecurity/

[36] See www.itu.int/

The Council of Europe

The Council of Europe Convention on Cybercrime was adopted in 2001,[37] and entered into force on July 1, 2004. By ratifying or acceding to the Convention, States agreed to ensure that their domestic laws criminalize the conducts described in the substantive criminal law section and establishes the procedural tools necessary to investigate and prosecute such crimes. The section on substantive criminal law contains of offences covering attacks against the critical information infrastructure of computer data, networks and systems.[38] The provisions of procedural law shall apply on any criminal offence committed by means of a computer system, and to the collection on evidence in electronic form of a criminal offence. The provisions contain expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of stored computer data, real-time collection of traffic data, interception of content data, and jurisdiction.

The 2005 Council of Europe Convention on the Prevention of Terrorism[39] was based on the need to strengthen the fight against terrorism, the rule of law, human rights and fundamental freedoms. The Convention was opened for signature in May 2005, and will enter into force on June 1, 2007. The principle of "extradite or prosecute" is especially included in Article 18.

A Recommendation was adopted on January 2007 for a co-operation against terrorism with Interpol.[40] It recommends that governments use the tools offered by Interpol against terrorism: the global police communications system I-

---

[37] See http://conventions.coe.int
The total number of signatures not followed by ratifications are 24, and 19 States have ratified the Convention (April 2007). An Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems of January 2003 has also been adopted.

[38] Article 2 - Illegal access:
…the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.
Article 3 - Illegal interception:
…the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.
Article 4 - Data interference:
…the damaging, deletion, deterioration, alteration or suppression of computer data without right.
Article 5 - System interference:
…the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data
Article 6 - Misuse of devices:
…the production, sale, procurement for use, import, distribution or otherwise making available of: a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2-5; a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Article 2-5, and b. the possession of an item referred to in paragraphs (a) (1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2-5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
Each country may reserve the right not to apply Article 6, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph a.ii of this article.

[39] See conventions.coe.int. The total number of ratifications/accessions is 6, and signatures not followed by ratifications are 33 (April 2007).

[40] Recommendation Rec (2007) 1 of the Committee of Ministers to member states regarding co-operation against terrorism between the Council of Europe and its member states, and the International Criminal Police Organization (ICPO – Interpol). See www.coe.int

24/7, the relevant databases and the real-time, operational support for police services.

G8 Group of States

The G8 Group of States established in 1997 a Subgroup on High-tech Crime and adopted ten principles in the combat against computer crime. The goal was to ensure that no criminal receive "safe havens" anywhere in the world. This Subgroup established the 24/7 network, which is an effective assistance on cybercrime and terrorism in cyberspace investigation and preserving electronic evidence, among almost 40 participating States.

The annual meetings have since then discussed both cybercrime and terrorism. In a joint communiqué at the 2004 Meeting of G-8 Justice and Home Affairs Ministers,[41] the States expressed that in order to combat terrorists and criminal misuse of the Internet, all countries must continue to improve the criminal laws. With a reference to the Council of Europe's Convention on Cybercrime, States were encouraged to adopt the standards and principles contained in the convention, and allow for more efficient law enforcement cooperation.

At the 2006 Moscow Meeting the G8 Justice and Home Affairs Ministers had further discussions on combating terrorism, cybercrime and issues of cyberspace and the necessity of improving effective countermeasures. The 2006 G8 Summit was held in St. Petersburg, and a Summit Declaration on Counter-Terrorism[42] reaffirmed the commitment on implementing and improving the international legal framework on counter-terrorism. The statement included effectively countering attempts to misuse cyberspace for terrorist purposes, covering incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists.

European Union

In the European Union a Council Framework Decision on attacks against information systems entered into force in 2005. This framework decision includes illegal access to information systems, illegal system interference and illegal data interference.[43]

---

[41] See www.usdoj.gov/ag/events/g82004/index.html

[42] G8 Information Centre, University of Toronto, Canada, see www.g7.utoronto.ca

[43] Article 2

Illegal access to Information systems

1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases that are not minor.
2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.

Article 3 Illegal system interference

Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.

The Justice and Home Affairs Council approved the European Union Counter-Terrorism Strategy in 2005. It emphasize that fight against terrorism is one of the greatest challenges of today. The Strategy commits the European Union to combat terrorism globally, while respecting human rights, and to make Europe safer, allowing its citizens to live in an area of freedom, security and justice. The Strategy is divided in four pillars: prevent, protect, pursue and respond.[44] One of the key priorities is to develop common approaches to spot and tackle the misuse of the Internet.

Asian Pacific Economic Cooperation (APEC)

The Ministers and Leaders of the Asian Pacific Economic Cooperation (APEC) have since 2002 [45] made commitments to endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and the Council of Europe Convention on Cybercrime.[46] The APEC Telecommunications and Information Working Group Meetings have made similar recommendations.[47]

The APEC Counter Terrorism Actions Plans was developed in 2003, and the Counter-Terrorism Task Force (CTTF) established in February 2003 with a mandate ending until 2008. The CTTF coordinates the implementation on statements and commitments on fighting terrorism, and assists member States on counter-terrorism capacity building. The aim of the CTTF is to coordinate APEC´s response to terrorism; to facilitate cooperation between APEC working groups and committees on counter-terrorism issues, capacity building and technical assistance programs. The programs will enhance cybersecurity and facilitate the investigation of cybercrime and terrorism.[48]

At the Ministerial Meeting in November 2005, APEC Ministers approved an APEC Strategy to ensure a trusted, secure, and sustainable online environment.

Article 4 Illegal data interference
Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor.

[44] See http://ec.europa.eu

"Prevent
Under this heading the EU aims to prevent people turning to terrorism by tackling the factors or root causes which can lead to radicalisation and recruitment, both in Europe and internationally.
Protect
Protection of citizens and infrastructures is essential. In its actions the EU seeks to reduce our vulnerability to attacks, through improved security borders, transport and critical infrastructure.
Pursue
The objective of the Union is to pursue and investigate terrorists both within the EU and globally. It is crucial to impede terrorist planning, travel, and communications. Terrorist networks should also be disrupted by cutting off the supply of both financial finding and operational materials. More generally, the aim is to bring terrorists to justice.
Respond
When Prevention, Protection and Response fail, we have to be prepared, in the spirit of solidarity, to manage and minimise the consequences of a terrorist attack. This can be done by improving capabilities to deal with the aftermath, the co-ordination of response and the needs of victims."

[45] See www.apectelwg.org

[46] See www.apecsec.org.sg/apec/ministerial_statements/annual_ministerial/2004_16th_apec_ministerial.html

[47] See www.apectelwg.org/e-securityTG/index.htm

[48] Makarim Wibisono, Ambassador and Chair CTTF: APEC´s Strategy to Support International Law Enforcement Cooperation to Counter Terrorism in the Asia-Pacific Region, Bali 2004. See www.apec.org

The member States was encouraged to fight the misuse, malicious use and criminal use of cyberspace by establishing legal and policy frameworks on substantive and procedural legislation, and mutual legal assistance arrangements.

Organization of American States (OAS)

The Organization of American States (OAS) established in 1999 a group of governmental experts. The group should prepare for Inter-American legal instruments and model legislations in combating cybercrime.

The Inter-American Convention Against Terrorism was adopted in 2002[49] in the aftermath of the 9/11 attacks in New York. Terrorism offences are the offences established in the 10 international instruments listed in Article 2. This convention entered into force in 2003.[50] An Inter-American Committee on Terrorism (CICTE) has also been established.

In 2005 a conference was organized[51] in cooperation with the Council of Europe and Spain, titled: *Cybercrime: A Global Challenge, A Global response.* Among the conclusions was adopted, that States was encouraged to consider the possibility of becoming Parties to the Council of Europe Convention on Cybercrime in order to make use of effective and compatible laws and tools at domestic level and on behalf of international cooperation. It was recognized the need of pursuing cooperation, providing technical assistance and organizing similar events in other global regions. The Sixth Meeting of Ministers of Justice in June 2006 confirmed this commitment.

The Commonwealth Model Legislation

In an effort to harmonize computer related criminal law in the Commonwealth countries, experts gathered together and presented a model law at a Ministers Conference in 2002. The model law is titled "the Computer Related Crimes Act"[52] and shares the same framework as the Council of Europe Convention on Cybercrime, in order to limit conflicting guidance. The model law serves as an example of common principles each country can use to adapt framework legislation compatible with other Commonwealth countries.

A "Model Legislative Provisions on Measures to Combat Terrorism." was developed in 2002 in order to assist the member countries to implement the United Nations Security Council Resolution 1373 (2001). The model legislative provisions has a definition of "terrorist acts" that includes an act or threat of action which "is designed or intended to disrupt any computer system or the provision of services directly related to communications infrastructure, banking or financial services, utilities, transportation or other essential infrastructure"

---

[49] See AG/RES. 1840 (XXXII-O/02) adopted on June 3, 2002, www.oas.org

[50] Samuel M. Witten, Deputy Legal Adviser, US Dept. of State: Testimony before the Committee on Foreign Relations, US Senate, June 17, 2004.

[51] See www.oas.org/juridico/english/cyber_meet.html

[52] Legal and Constitutional Affairs Division, Commonwealth Secretariat, available at http://www.thecommonwealth.org

Association of Southeast Asian Nations (ASEAN)

The Association of Southeast Asian Nations (ASEAN)[53] has established high level Ministerial Meetings on Transnational Crime. At the Meeting in 2004, a statement included cyber crime was recognized and the need for an effective legal cooperation to enhance the fight against transnational crime.

A Plan of Action to Implement the Joint Declaration on ASEAN-China Strategic Partnership for Peace and Prosperity was signed in 2003. ASEAN and China made a statement on joint actions and measures, including cooperation for preventing and combating cybercrime and enhancing cybersecurity.

An ASEAN Regional Forum Seminar on Cyber-terrorism was held in 2005 and national policies were discussed. A statement from the Regional Forum was made in 2006 and emphasized the need for a rapid and well functioning legal cooperation in the fight against cyberattacks and terrorist misuse of cyberspace. Member States should implement cybercrime and cybersecurity laws in accordance with their national conditions and by referring to international instruments, recommendations or guidelines for the prevention, detection, reduction, and mitigation of attacks. National frameworks for cooperation and collaboration in addressing criminal misuse of cyber space, including terrorist, acts was emphasized and encouraged.[54]

The Organization for Economic Co-operation and Development (OECD)

The Organization for Economic Co-operation and Development (OECD)[55] adopted in 2002 new "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security." This approach to the critical information infrastructure protection is a guideline, and as such not binding for member States. It is the product of a consensus between OECD governments.[56] The Guidelines was adopted in order to counter cyberterrorism, computer viruses, hacking and other threats.

An OECD Global Forum on Information Systems and Network Security was held in 2003, and a workshop on Cybercrime was also organized in conjunction with the Forum.

A Working Party on Information Security and Privacy released in 2005 a report "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries and provided a web site.[57] The report included a survey of member States national initiatives to implement the 2002 Guidelines. Among the main findings was that almost all States had adapted legal frameworks on fighting cybercrime and that the protection of the national critical information infrastructure was a main area for developing a culture of security.

---

[53] ASEAN Group consists of 10 States: Brunei Darussalam; Cambodia; Indonesia; Laos; Malaysia; Myanmar; Philippines; Singapore; Thailand; Viet Nam, see www.aseansec.org

[54] See ASEAN Regional Forum Statement on cooperation in fighting cyber attack and terrorist misuse of cyberspace (June 2006).

[55] See www.oecd.org

[56] See also Isabelle Abele-Wigert and Myriam Dunn: International CIIP Handbook 2006 Vol. I.

[57] See www.oecd.org/sti/cultureofsecurity

And almost all the member States had established national Computer Security Incident Response Teams (CERT).

NATO

NATO[58] has also been active on civil emergency planning. The Senior Civil Emergency Planning Committee (SCEPC) assists member States in the protection of civilian populations from terrorist attacks against critical infrastructure. And the responsibility for coordinating the civil critical infrastructure protection lies with the SCEPC.[59]

The Civil Communication Planning Committee (CCPC) is responsible for the electronic public and non-public communication infrastructures, and has published several papers on civil communications infrastructures. It has also contributed with papers on consequences regarding cyber-attacks and information warfare on critical civil communication infrastructure. The Civil Protection Committee (CPC) has initiated work on critical infrastructure protection, and has developed a Critical Infrastructure Protection Concept Paper in 2003. Recently the CPC organized a seminar on Critical Infrastructure Protection (CIP) – Education"

Threat from terrorism to critical infrastructure was discussed at the NATO Summit in 2002 and a NATO Cyber Defence Programme was implemented. NATO Communication and Information Systems Services Agency (NCSA) have been established as NATO´s first line of defence against cyber terrorism. The NATO Information Security Centre (NITC) is the operational centre.[60]

Protection of Individual Rights

Three of the principle sources of these fundamental individual rights are the Universal Declaration on Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms. These documents support the right of every person to exercise the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media regardless of frontiers, as set forth in Article 19 of the Universal Declaration of Human Rights.

Council of Europe Convention on Cybercrime, Article 15, addresses the requirements for safeguards on individual rights and provides categories where procedural protections are most necessary, especially the principle of proportionality.

Conclusion

None of the publicly known incidents today qualify as terrorism in cyberspace, and the threat of terrorism in cyberspace is still potential. But it must always be

[58] See www.nato.int
[59] See Isabelle Abele-Wigert and Myriam Dunn: International CIIP Handbook 2006 Vol. I.
[60] See www.nato.int/ncsa/topics/combating_cyber_terrorism.htm

a reason to be precaution and to prevent against, to the same extent as the protection of critical information infrastructures. When implementing preventing efforts one should always have in mind that the fight against terrorism in cyberspace is not a war, but a fight against cybercrime.

The 9/11 attacks in New York caught the world by surprise, and so could a coordinated major cyberattack. The threat of terrorism in cyberspace may be exaggerated, but we can neither deny it nor dare to ignore it.[61]

Terrorist acts in cyberspace may still be a myth, but the use of cyberspace as public provocation, recruitment and training for terrorist acts is a reality. Public provocation, recruitment or training for terrorist acts, such as in the Danish case, could only be the future terrorism in cyberspace. Cyber attacks do not cause similar fear as the destruction of tangible property. Cybersecurity measures will also always include back-ups, which restore the data immediately or within some hours.

[61] See Gabriel Weinmann: Cyberterrorism-How Real is the Threat? United States Institute of Peace (2004), see www.usip.org