

# GENTIUM

Vol. 3 (9), October 2008



Public International Law Students United

---

*There's Something About Cyberterrorism*

by Yaroslav Shiryayev

pp 3-4



### **There's Something About Cyberterrorism**

No discussion of terrorism can make do without eventual mention of the lack of common definition. To make it short, in my opinion, the concept of terrorism cannot exist without 3 basic elements: fear, violence and civilians (non-military aircraft / ship crew and persons falling under the effect of the Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, should also be considered civilians). An offence can only be called an act of terror, if its consequences instill sufficient amount of fear in civilian population. Violence (or at least perceivable remote possibility thereof) is a crucial component of intimidation, as physical violence is the only thing capable of making civilians experience the feeling of *terror*. Therefore, terrorism is violence aimed at inspiring fear and intimidating population. The same conclusion can be made if one combines for example Council of Europe Parliamentary Assembly's Recommendations 1426 (par. 5) and 1706 (par. 2).

Following a simple grammatical legal interpretation, the word "terrorism" stands for a "process of being engaged in an act of terrorism". Furthermore, a person cannot be called a terrorist until he has been directly engaged in the act of terror, an expression "potential terrorist" should be used instead. A suicide bomber retains his "potential terrorist" status until he either attempts to trigger the explosive or reveals his belt to the audience around him (who in turn embrace the danger), thus legally turning into a real "terrorist" (from that point there is no "going back", the status change is permanent). While terrorism cannot be considered such without acts of terror, legally it is possible to resort to terrorist (*adj.*) methods without being a "terrorist". Let's call this phenomena "quasi-terrorism". Hijacking a small civilian aircraft with low fuel and without anyone on board in a region, where it cannot be used as a weapon (e.g. the Antarctic) can be considered an example of such quasi-terrorism (since the plane is incapable of causing violence, it does not frighten civilians, thus, seizure of the aircraft cannot be considered an act of terror). Following the logic, resorting to terrorist methods can be called a terrorist offence. Every act of terror is a terrorist offence, but not every terrorist offence falls under the concept of terrorism. My hat goes off to whoever in CoE's CODEXTER decided to turn down Pace's proposal (in Recommendation 1550) to adopt "definition of terrorism" as it stands in the European Council

Common Position of 27 December 2001 (which mistakenly lists certain cases of quasi-terrorism as acts of terrorism), and suggested replacing it with “terrorist offences”.

Moving on to the topic of cyberterrorism, first of all it should be said that dissemination of racist and xenophobic material has absolutely nothing to do with terrorism whatsoever. The idea that it serves the terrorist cause is dubious and the act itself does not even come close to a terrorist offence. Worth criticism are also Sieber’s ideas that propaganda, fundraising, financing, individual communication, virtual damage, acquisition of satellite images and construction plans should be included in the concept of cyberterrorism. Even some names of books today are misleading, e.g. “Cyberterrorism – the use of the Internet for terrorist purposes”. As with “normal” terrorism, cyberterrorism is merely a process of being engaged in the act of cyberterrorism (i.e. an act, which is carried out in the cyber-space, and that threatens violence to civilians in the physical world, thus instilling terror in their minds); preparations for terrorism cannot legally be considered terrorism *per se*. This is unacceptable primarily from the legislative point of view, as it would give illegal propaganda and other lesser-offences the same gravity as certain grave crimes, e.g. violent assaults against human beings.

What concerns threats in the virtual world, they must first of all amount to cyber-acts of terror, that is they must instill fear on subjective level. Example: a video is uploaded on YouTube, where presumably a tourist was violently beaten and stabbed to death, followed by a threatening message, stating that all country X’s nationals will meet the same fate. If this video will be viewed by a sufficient portion of citizens of state X and perceived as a real danger to their lives, such threat can amount to cyber-act of terror, irrespectively of whether cyber-terrorists intend to fulfill the promise or not and whether this was real-life footage or just a performance.

Cyber-acts of terrorism (in whatever form, be it tweaking hospital systems or unleashing radiation by overheating a nuclear reactor) are indeed possible if they lead, can lead or threaten to lead to physical damage to health of civilians. Attempt and participation in such acts should obviously be punishable, but not as cyber-crimes, rather as cyber-acts of terror. Once again, from legislative perspective, cyberterrorism and simple cyber-crimes cannot be considered equal. Finally, I don’t agree that CoE Convention on Cybercrime “deals with cyberterrorism by means of a “data approach””, truth is: it does not deal with it at all, more importantly, it should not, since cyber-acts of terrorism and small-time cyber-crimes are obviously offences of different caliber.