Cyberattacks, Cyberterrorism and Cyber-use of Force: Countering the Unconventional under International Law

Aris L. Gulapa

48 ATENEO L.J. 1051 (2004)

SUBJECT(S): *INTERNATIONAL LAW, TERRORISM, CYBERTERRORISM, CYBERATTACKS, USE OF FORCE, RIGHT TO SELF-DEFENSE*

KEYWORD(S): *INTERNATIONAL LAW, TERRORISM, CYBERTERRORISM, CYBERATTACKS, USE OF FORCE, RIGHT TO SELF-DEFENSE, ELEMENTS OF CYBERTERRORISM, STATE SECURITY, STATE RESPONSE TO TERRORISM*

This Note starts with a description of the events surrounding the Information Age, focusing on the post-September 11 cyber attacks and the enactment of the Philippine E-Commerce Act, and of the threat of computer-based attacks to State security, ending with the question of what lawful responses are available to the State.

The Author differentiates between conventional terrorism and catastrophic terrorism in his attempt to discuss the crime of terrorism and how the cyber age changes its definition, especially with the existence of the crime of hacking. The Philippine definition of cyber terrorism is then analyzed with respect to State practice, *opinio juris*, G.A. Resolution 53/70, which is a resolution on cyber activity in relation to state security, and House Bill 3802, which provides for a definition and penalties for the crime of cyber terrorism. He then states the following elements which constitute the crime of cyber terrorism and discusses each element individually: 1) The cyber attack must be against critical infrastructure computer systems causing severe harm or violence to civilians; 2) It must be politically motivated; and 3) The attack should create a state of terror in the minds of the general public or segment of a population. Acts which fall short of the definition of cyber terrorism are also noted, such as harmless or non-politically-motivated cyber activities.

Finally the Author submits that a cyber attack upon a State constitutes a prohibited use of force, which will trigger a State's right to self-defense, even if such attack had already taken place, provided that such State response is proportional and necessary. He then evaluates and recommends the proper State responses to cyber activisim, hactivism, or cyber terrorism by individuals or under state participation.