

Terrorist attacks can be prevented by the advanced IT

Student Name:

Mr. Seongtaek Im

Asia-Pacific Homeland Security Student Fellow

East West Center at University of Hawaii

Conference Mentors:

Mr. Russ Johnson

Homeland Security Industry Manager / ESRI, Inc

Mr. Royce Jones

Hawaii Pacific Manager / ESRI, Inc.

Terrorist attacks can be prevented by the advanced IT

During the last two decades, the Information Technology has had a significant impact on the global terrorism. The advanced IT has permitted terrorists to have easy access to government information, recruit young operatives, influence others about their beliefs, and carry out their terrorist activities. IT networks can also offer targets for terrorists who aim to destroy public network infrastructure by launching cyber-attacks. But IT can also be exploited by international intelligence agencies as a counterterrorism, if they are willing to work together by sharing the information. It can support the monitoring planned attacks in the various places and any time now.

IT allows terrorist groups to spread their ideology and facilitates recruitment. The terrorist are using the cyberspace and its technology such as website, internet messaging system, cyber-communities, and chat rooms spreading their messages or propaganda. It could be used for a brain wash training and misleading the young people, recruitment, internet money transferring and garnering support. The Internet is influencing the radicalization of young people by spreading propaganda and showing videos of executions of

hostages, successful terrorist attacks.

The terrorist used the Internet to make a plan for their operations by transferring the money for the operations, booking air tickets online and communicating with one another through Internet messaging system and in the chat rooms. Some terrorist groups can have easy access and use sophisticated technological devices such as optoelectronics, encrypted communications equipment, GPS systems, and remote electronic bomb detonators. Here again, law enforcement personnel are handicapped by the accessibility, versatility, speed, and transnational character of cyberspace, which allows almost total impunity.

Prior to any potential terrorist attack, the international intelligence services rely heavily on Internet use to identify significant patterns of behavior among suspected individuals and groups. Cyber monitoring system have been developed for modeling the progress of social groups in cyberspace such as chat rooms, internet communities, newsgroups, and internet boards, with the specific goal of detecting potentially dangerous terrorist groups.

The international community needs to improve the international law enforcement cooperation. International intelligence agencies are required to

have the same view on measures that would be both efficient and acceptable in terms of privacy, such as improving the accessibilities on the internet, extending log files control rules for Internet service providers (ISP), and advanced monitoring systems for elasticity of Internet protocols address. Some progress has already been made in raising awareness of false usage of IT and its risks, but there is a need for more international cooperation in developing the advanced security of cyberspace, and promoting efficient international law enforcement together.