ORIGIN IO-00

INFO LOG-00 EEB-00 AMAD-00 CIAE-00 INL-00 DODE-00 DOTE-00
PDI-00 DS-00 DHSE-00 OIGO-00 E-00 FAAE-00 FBIE-00
UTED-00 VCI-00 FOE-00 FRB-00 TEDE-00 INR-00 JUSE-00
L-00 MFLO-00 MOFM-00 MOF-00 VCIE-00 NEA-00 DCP-00
NSAE-00 NSCE-00 OIC-00 OIG-00 NIMA-00 PA-00 PER-00
GIWI-00 P-00 SCT-00 DOHS-00 SP-00 IRM-00 SSO-00
SS-00 TRSE-00 ASDS-00 FMP-00 CBP-00 R-00 IIP-00
SCRS-00 DSCC-00 PRM-00 DRL-00 G-00 SAS-00 FA-00
/000R

089049
SOURCE: CBLEXCLS.005383
DRAFTED BY: IO/PSC:CMFANCHER -- 08/19/2008 202-736-7734
APPROVED BY: IO:BHOOK
IO/FO: EGOLDRICH - OK
IO/PSC: RMORAN - OK
IO/UNP: MGARUCKIS - OK
S/P: DTWINING - OK
P: AREINEMEYER - OK
D: JCKELLEY - OK
S/CT: RFALLON - OK
NEA/RA: LGOTTLIEB - OK
IIP/CTCC: TRECEVEUR - OK
----------C96E6B 191738Z /38
P 191730Z AUG 08
FM SECSTATE WASHDC
TO USMISSION USUN NEW YORK PRIORITY

UNCLAS STATE 089049

E.O. 12958: N/A
TAGS: PTER
SUBJECT: USUN INSTRUCTION: U.S. INPUT FOR UN WORKING GROUP ON COUNTERING THE USE OF THE INTERNET FOR TERRORIST PURPOSES

1. This is an action request. USUN is requested to please submit the U.S. response below to the UN CTITF Working Group on Countering the Use of the Internet for Terrorist Purposes.

2. BEGIN TEXT:

U.S. Input for the UN CTITF Working Group on
Countering the Use of the Internet for Terrorist Purposes

Overview of U.S. perceived challenges posed by terrorist use of the internet:

Exploitation of the Internet,s various capabilities by terrorists has increased dramatically in recent years. The Internet has facilitated al-Qa'ida,s transition from a centrally-managed organization to a more diffuse movement, while other terrorist, insurgent, and extremist groups have

embraced the Internet as a key tool, exploiting its relatively simple nature and widespread availability.

Many of the Internet's features are valuable to terrorist organizations: the vast information available on the World Wide Web permits research on weapons, tactics, and potential targets; a superior communications network facilitates information sharing among members, propaganda dissemination, indoctrination and training, fundraising, and radicalization of new or potential recruits. The internet provides terrorists a means of conducting some of these activities clandestinely.

We assess that a key use of the Internet by terrorists involves email, because it is a simple, widely available vehicle for communicating. Many terrorists employ a variety of methods to conceal their activities, such as coded language that disguises the nature of the content, or using public Internet cafes to hinder efforts to identify users.

An al-Qa,ida training manual discovered in Afghanistan after the fall of the Taliban regime states "using public sources openly available, it is possible to gather at least 80 percent of all information required about the enemy." We suspect that terrorists routinely use the Internet to gather intelligence on prospective targets and to gain insight into counterterrorism security measures that are in effect. Many radical extremists who may turn to violence and terrorism are young, educated men who are technologically savvy, and thus probably proficient in mining data from the Internet. They are also increasingly able to educate themselves and train others on terrorist weapons and tactics via the Internet--for example, step-by-step instructions for making acetone peroxide, the explosive used in the July 7, 2005 London bombings, and many other explosives and poisons, can be found online.

Al-Qa'ida and its associated movements consistently use the Internet as a means of disseminating propaganda. Al-Qa'ida in Iraq (AQI) has been particularly aggressive in this regard, using the Internet to broadcast beheadings of hostages and to publicize videos showing attacks against United States and coalition forces in Iraq. AQI's media wing also has become adept at memorializing suicide bombers and spreading radical ideology. Al-Qa'ida's senior leaders also have increased their use of the Internet to broadcast propaganda, such as deputy leader Ayman al-Zawahiri's audio and video messages--which are increasingly sophisticated and nearly professional in quality.

We have seen terrorists use multiple websites and online forums to post proclamations, to mobilize followers, and to recruit new members, particularly following events they believe will generate support for their cause. We observe spikes in online activity following highly publicized events, like the publishing of cartoons that depicted the prophet

Muhammad, or military conflicts involving Muslims such as the 2006 conflict between Israel and Hizballah, and the Iraq war.

We lack information to judge how effective these efforts have been, but we believe that some individuals have been motivated to join radical extremist movements or provide money or other support to terrorist groups as a result of online efforts.

1. Legal Measures aimed at criminalizing and policing the use of computer systems to carry out cyber attacks:

While no U.S. law explicitly defines or criminalizes "cyberterrorism," or the use of a computer system to carry out a terrorist attack, a number of U.S. statutes can be used to investigate and prosecute the underlying criminal cyber conduct. For example, United States law prohibits accessing a computer system without authorization or in excess of authorization. Commonly referred to as a "hacking" law, this statute can be used to target perpetrators who, among other things: unlawfully access a computer to obtain national security information from the United States, or who cause damage to a computer system which results in a special harm. In the terrorism context, that special harm may include: the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals; physical injury to any person; a threat to public health or safety; or damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security. Moreover, hacking activities can also fall under the federal crime of terrorism when national security information or one of the special harms enumerated above is present, and the prohibited conduct is intended to influence or affect the conduct of the government by intimidation or coercion, or to retaliate against government conduct. Under those circumstances, this computer-related conduct may be eligible for inclusion as a target offense in the material support statutes, discussed below, as well as subject to an extended statute of limitations.

In addition to the hacking law, which would criminalize an actual terrorist cyber attack against the critical infrastructure, other U.S. laws could be used to target terrorists engaged in cyber criminal activity. Traditional laws targeting terrorist conduct, like the U.S. law prohibiting conspiracy to kill, kidnap, maim, or destroy property, can be applied to terrorists using cyber methods to perpetrate their offenses. But more broadly, some other U.S. laws could be used to target the criminal cyber conduct of terrorists, including laws criminalizing identity theft, other computer-based fraud, access device fraud, wire fraud, or the unlawful interception of communications, as well as general laws criminalizing conspiracy and aiding and abetting.

Depending on the specific facts and circumstances, these criminal laws and other civil and administrative (non-criminal) tools may be applicable to conduct that occurs on a protected computer system. These laws could be used to prosecute the terrorist perpetrators of cyber-based attacks against the critical infrastructure or other criminal cyber attacks.

2. Legal measures relevant to the issue of terrorist planning or the dissemination of terrorist content, for example incitement to carry out terrorist attacks, the propagation of terrorist training material or the seeking or transfer of funding for terrorism:

The content of Internet websites hosted in the United States is protected by the free speech guarantee of the First Amendment to the U.S. Constitution, which provides that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." (U.S. Const. Amend. I.) The free speech guarantee of the First Amendment has been interpreted by the U.S. Supreme Court to extend to speech advocating illegal conduct, and regulation of such speech is permissible only in narrow circumstances: "the constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation, except where such advocacy is directed to inciting or producing imminent lawless actions and is likely to incite or produce that action." Speech that is tantamount to conduct, however, or that is simply the means of effecting conduct, may be legitimately proscribed, punished, or regulated incidentally to the constitutional enforcement of generally applicable statutes. A number of U.S. statutes criminalize speech-related conduct in certain circumstances, including general laws criminalizing the solicitation to commit acts of violence, conspiracy, and aiding and abetting. More specific laws forbid such acts as seditious conspiracy; advocating the overthrow of the government; conspiring within the jurisdiction of the United States to kill, kidnap, or maim any individual outside the United States or in a foreign country with which the United States is at peace; teaching the manufacture or use of explosives, destructive devices, and weapons of mass destruction; mailing material that incites murder, assassination, or arson; and providing material support or resources to terrorists or to designated terrorist organizations.

The U.S. material support laws are broad-based charging statutes that provide an important vehicle for prosecuting terrorists' recruitment, training, and fundraising efforts, which is sometimes conducted by terrorists online. Material support or resources may include actions such as providing

funding, training, expert advice or assistance, personnel, or providing communications equipment (which could include ISPs and other web access or services, among other things). The material support provisions, however, either require proof that the defendant knew or intended that the support was to be used in the preparing or carrying out of a terrorist activity, or proof that the defendant knowingly provided material support to a designated foreign terrorist organization, regardless of whether the defendant knew that the support would be used for a terrorist activity. Additionally, U.S. law also prohibits certain financial transactions with certain designated foreign states or entities, or individuals.

Depending on the specific facts and circumstances, these criminal laws and other administrative (non-criminal) tools may be applicable to unlawful conduct that occurs on a U.S. website, and could be used to close U.S. websites being used to facilitate criminal activity. However, any prosecution for speech-related conduct on the Internet would face significant First Amendment, due process, and other statutory challenges.

3. Measures for protecting human rights online and ensuring the freedom of access to the internet in the context of attempts to combat terrorist use of the internet:

The United States strongly supports and defends freedom of expression and the free flow of information on the Internet. Protecting free speech rights online and ensuring the freedom of access to the Internet are fundamental U.S. values embedded in our most basic laws and the First Amendment to the U.S. Constitution. Only in narrow circumstances, as described in our response to question two above, may this right be legitimately proscribed, punished, or regulated.

4. Projects aimed at exploring and researching the dimensions of the online terrorist threat:

The U.S. Government monitors publicly available material on the Internet. The U.S. Government reads and reviews information posted on the Internet by both international and domestic terrorist groups, consistent with U.S. law, in order to properly protect the U.S. homeland against terrorist attack. U.S. Government agencies and state and local law enforcement organizations have obtained valuable information on terrorist groups based in part on review of publicly-available information on terrorist websites. Additionally, Federal, state and local law enforcement agencies may during the course of a criminal investigation read and gather information from websites that promote violations of U.S. law such as violent crimes, money laundering, or material support to terrorists. The impetus for doing so often is an ongoing criminal investigation. The U.S. Government may, consistent with U.S. law, review websites that promote violence or terrorism against U.S.

citizens.

5. Projects (online or otherwise) aimed at countering the ideology of terrorist groups that is propagated over the internet:

The U.S. Government reads and reviews information posted on the Internet by both international and domestic terrorist groups, consistent with U.S. law. Federal, state, and local legislatures and regulatory bodies that oversee the work of intelligence and law enforcement organizations ensure that organizations charged with monitoring terrorist websites are provided with appropriate resources and guidance.

Evidence shows that moderate voices can influence and counter radicalization and recruitment by helping to reverse the spread of extremist ideology. We are committed to developing effective tools to better understand the motivations of those who join or support terrorist networks, as well as the incentives and recruitment techniques employed by terrorists. We employ all elements of U.S. national power, including public diplomacy, educational opportunities, development initiatives, and democracy-building programs, to address the underlying social and economic conditions terrorists exploit and to counter extremist propaganda and recruiting.

Our public diplomacy work is guided by three strategic imperatives: 1) to offer a positive vision of hope and opportunity rooted in the U.S. commitment to freedom and democracy; 2) to promote the fundamental and universal rights of free speech and assembly, the freedom to worship, the rule of law, and rights for women and minorities; and 3) to isolate and marginalize violent extremists and undermine their efforts to exploit religion to rationalize their acts of terror. We advance these strategic objectives by engaging foreign publics to explain and advocate American policies and ideology, and to counter extremist rhetoric and disinformation coming from hostile groups.

The U.S. State Department maintains a public "Identifying Misinformation" website, in English and Arabic, devoted to countering false stories that appear in extremist and other web sources. The site focuses on disinformation likely to end up in the mainstream media. U.S. Embassies have used information from this site to counter disinformation in extremist print publications in Pakistan and other countries. One article, "A Trio of Disinformers," was the subject of a 1,100-word front-page article in an issue of the influential pan-Arab newspaper al-Sharq al-Awsat. "Identifying Misinformation" is featured on the America.gov website, and is listed first of 17.6 million sites in a Google search for the term "misinformation." At least 49 websites have direct links to it. The State Department's web page to explain U.S. counterterrorism policy is featured on http://America.gov. The site is listed third out of 241 million sites in a Google search for the terms "terrorism U.S." At least 133 websites

link directly to it.

The Digital Outreach Team (DOT) is another U.S. State Department effort to explain U.S. policies and counter violent extremist ideology on the internet. Beginning operations in November 2006, the team operates openly as part of the State Department and focuses its engagement with mainstream-not militant - sites. The DOT has posted at least once on some 75-80 sites but concentrates on two dozen sites at present. The team posts around 30-35 products a week of varying lengths (one paragraph to several pages). Weekly viewership of DOT materials can be measured in the thousands of persons or even much larger for the occasional on-the-air readings by BBC Arabic radio and television of DOT postings to the BBC website. DOT materials are sometimes reproduced in print copies of newspapers.

The DOT responds to the generally hostile or skeptical reception it encounters online by relying heavily on facts and objective analysis. It focuses arguments away from historical grievances towards shared values and a search for common ground in resolving current problems. The DOT makes frequent reference to U.S. society, its political system and values since misinformation about these areas is frequently transposed into misperceptions about U.S foreign policy. A key challenge faced in shaping DOT messages is distorted (and widely held) views of what motivates U.S. policies.

The Counterterrorism Communications Center (CTCC) was created in mid-2007 as an interagency center, housed in the U.S. State Department, reporting directly to the Under Secretary of State for Public Diplomacy and Public Affairs. It was created to take the lead on international strategic communications for countering ideological support for terrorism within the Administration. One of the CTCC deliverables is the development and distribution of counterterrorism Themes and Messages for the foreign policy, defense and security communities. The Themes and Messages product currently reaches more than 2000 subscribers including every Embassy, Combat Commanders and associated State Department staffs and is used by communicators abroad and in Washington on various internet forums, public engagements, speeches, newspaper opinion pieces, and private discussions. The CTCC has also launched Internet initiatives and digital outreach programs that take the fight to the terrorist information battleground through Arabic, Persian, and Urdu websites, podcasts, video production and distribution, and other communication tools such as cell-phones and low-bandwidth video tools.

6. Information sharing and online training projects for agencies involved in counterterrorism:

Federal, state, and local legislatures and regulatory bodies that oversee the work of intelligence and law enforcement organizations ensure that organizations charged with

monitoring terrorist websites are provided with appropriate resources and guidance. Additionally, the Federal government encourages an information sharing environment among Federal departments regarding terrorist use of the Internet.

Note: This document represents a broad overview of USG efforts in countering the use of the Internet for terrorist purposes. It is not all inclusive and does not include State and Local government efforts or other important civil society efforts.

http://www.whitehouse.gov/nsc/nsct/2006/nsct2006.pdf
http://www.whitehouse.gov/pcipb/cyberspace strategy.pdf

END TEXT.

3. The Department appreciates the Mission's efforts.
RICE

NNNN

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu