STATEMENT OF

MICHAEL S. DORAN

DEPUTY ASSISTANT SECRETARY OF DEFENSE

SUPPORT TO PUBLIC DIPLOMACY

BEFORE THE COMMITTEE ON HOMELAND SECURITY

AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

3 May 2007

Mr. Chairman, members of the committee, I welcome the opportunity to testify today regarding the use of the Internet by terrorist organizations. The President has said that "the war against this enemy is more than a military conflict. It is the decisive ideological struggle of the 21st century, and the calling of our generation." While this struggle bears some comparison with past ideological conflicts, it differs in that the Internet allows relatively small organizations with limited resources, such as Al-Qaeda, to broadcast messages across the globe instantaneously. In past conflicts, only nation states could disseminate their messages so widely.

Terrorists are using the Internet now more than ever in an attempt to influence the global political environment. Al-Qaeda and its associates, in particular, use the Internet to

spread their political ideology, disseminate the extremist interpretation of religion that supports it, and coordinate their operations. The focus of my office's efforts is on foreign-language, insurgent websites believed to be operated by non-US persons. We work closely with the Department of State, the National Counterterrorism Center (NCTC), and other agencies to remain abreast of how our adversaries use this medium. Because individuals can access the Internet anonymously from virtually anywhere on the globe, the use of the web by terrorists is a constantly moving target.

Our deep commitment to a free society and the very nature of the web make it virtually impossible to prevent terrorists from using the Internet altogether. From a handful of terrorist web sites in 2000, today there are many thousands of terrorist-related websites in existence, with more appearing each week. Through the deft use of members-only user groups and password-protected bulletin boards, terrorist groups such as Al-Qaeda manage to maintain the integrity of their "brand," instructing sympathetic audiences as to the whereabouts of authoritative communications. At any given moment, in any given language, only a limited number of sites post original material produced directly by terrorist organizations or the religious authorities to whom the organizations have pledged loyalty. The majority of terrorist websites in operation are either mirrored versions of existing sites, or simply bulletin boards that disseminate material that originated on websites under the direct control of terrorist organizations.

Those characteristics that turned the Internet virtually overnight into an indispensable tool of our day-to-day life have also made it a boon to terrorist organizations: using the Internet is cheap; it allows the rapid dissemination of text, video, and audio files; and, importantly, it allows anonymous communications to very large

audiences. The benefits to terrorist groups of a cheap and anonymous multi-media communications system are obvious.

Terrorism experts have long analyzed terrorist attacks as a form of communication. A primary goal of the terrorist attack is to attract attention so as to disseminate information. In the 1970s, terrorism expert Brian Jenkins expressed this insight by famously remarking that "terrorists don't want a lot of people dead, they want a lot of people watching." In today's world, marked as it is by groups such as Al-Qaeda, it is no longer true that terrorist groups don't want a lot of people dead. It is, however, still very much the case that they want a lot of people watching. The Internet ensures that they have the means to communicate their message to the world immediately and directly, without being filtered through the prism of the mainstream media.

The anonymity of the web and the ready availability of a virtual space for posting material in large quantities make it easy for terrorist-related sites to pop up temporarily, publish new material, and then move to another address when necessary. Once the material has been published, it is immediately duplicated on a large number of sites located on servers across the globe. The speed with which this dissemination occurs poses a serious challenge to those in the U.S. government working to locate hostile sites, and assess their content.

In fact, the web has created conditions that make it possible for us to imagine a wholly new type of terrorist network – one that is almost entirely virtual – composed of individuals who are not personally known to each other but who are animated by the same ideology and willing to coordinate actions in pursuit of it.

In addition to easing communication, for some groups, terrorist use of the internet may increase the difficulties that law enforcement authorities face in tracking and apprehending potential terrorists. Added by the internet and other communication technology, terrorists can operate in a variety of different jurisdictions, each with their own specific laws and regulations governing the monitoring of the Internet and the prosecution of online crime.

Al-Qaeda and likeminded groups have a striking ability to obtain a large variety of multimedia products, rapidly repackage them to fit their own goals and objectives, and then make that data available to a global audience via the Internet. The Internet, therefore, is more than just a tool of terrorist organizations: it is the primary repository of the essential resources for sustaining the culture of terrorism. Terrorist organizations such as Al-Qaeda use the Internet for a variety of organizational purposes including propaganda dissemination, recruitment, fund raising, training and instruction, and operational planning.

But the Internet is more than an operational tool. It also houses hundreds of thousands of pages of books that define the extremist interpretation of religion that feeds the global terrorist movement. For instance, the followers of Abu Muhammad al-Maqdisi, who at one time served as the spiritual guide to Abu Musab al-Zarqawi, have compiled on a website dedicated to their mentor a considerable library of downloadable books that treat subjects covering all aspects of religious life. A large part of this material is devoted to debunking the moderate critiques of the extremist interpretation of religion. Sites such as this allow the Internet to function as a kind of virtual extremist madrassa.

Thanks to the Internet, terrorists now have direct control over their message and the means of disseminating it, with the ability to disburse their propaganda directly to sympathetic audiences without the filter of third-party media. Terrorists also post violent images, such as decapitation videos, to invoke fear and deliver threats. But intimidation, although it grabs attention, is not the main theme of terrorist propaganda, which more often than not generally focuses on the perceived wrongs that Muslims have suffered at the hands of non-Muslims, led by the United States. It also stresses the religious justifications for taking violent action against them as a matter of defense. Terrorist propaganda seeks to de-legitimize the adversaries of the extremists, to spread disinformation about enemy actions and intentions, and to bolster the morale of followers - all ultimately to persuade potentially sympathetic audiences that jihad is a fundamental component of religion and the only effective means for redressing grievances. .

The Internet can facilitate terrorist recruitment. Along with print materials, social influences, and other factors; potential recruits are flooded with propaganda, training manuals, and religious justification for joining the jihad via the Internet. It is difficult to say how much direct recruitment takes place on the web. While it is likely that direct invitations to take part in a terrorist organization are usually delivered face-to-face, there is no doubt that the web plays an important role in indoctrinating recruits before they are drawn in directly. Probably for this reason, extremist websites will not attempt to recruit overtly for violent action, but will instead legitimate the actions of terrorists and encourage readers to support the jihad however they can.

Terrorist websites, chat rooms, and other forums make use of the Internet for fundraising. These websites often use the argument that every Muslim has a duty to

support jihad, but that participation on the ground is not required of everyone. The appeal for financial support alone is a method of permitting an individual to feel that they have "done their duty" as a Muslim, but do not need to change their life and join the actual fight.

Terrorist use of the internet also includes operational training. For example, an online initiative, called "Jihad University," offers training information in the use of small arms, mortars, rockets, and artillery; guidance on where to fire at U.S. forces vehicles to inflict the greatest damage; sniper training; and detailed instructions about the construction of improvised explosive devices (IEDs), suicide vests, etc. Training also includes information on how, when, and where to cross the borders of Iraq to join the jihad, and how to avoid detection as a jihadist.

As I have endeavored to illustrate, terrorists use the Internet for a wide variety of purposes, and their use of the technology continues to evolve. I have provided the Committee with compact discs containing audiovisual material from some of these terrorist websites for those Committee members who are interested in seeing a demonstration of the some of the typical content found on these websites. The briefing on this CD was produced by the Department's contracted Center for International Issues Research (CIIR), an innovative center focused in part on observing terrorist activity on the Internet in order to provide policy makers and agencies with a greater understanding and awareness of the strategic communication campaigns being waged by extremist groups across cyberspace. CIIR was established precisely out of the recognition that Al-Qaeda and its affiliates use the internet quickly and effectively on a global scale. Such a threat

required a team ofanalysts capable of following the day-to-day expression of the extremist ideology across national and linguist barriers.

When recognizing the nimble use that Al-Qaeda makes of the internet, it is tempting to call for us to counter it directly on the net. Ultimately, the key to countering the terrorists' use of the internet is not simply or primarily a reciprocal set of actions by the U.S. government on the web. As the President has reminded us, we will counter the terrorist ideology most effectively by using the strongest weapon in our arsenal - the power of freedom. The Internet is a tool of a free society, and, as such, it can sometimes be used as a tool to undermine freedom. Nevertheless, the answer to the terrorist message of tyranny, intolerance and violent extremism is to effectively communicate the alternative vision: freedom, tolerance, and mutually-beneficial cooperation.

Precisely in order to address the challenges presented by the war of ideas and to communicate our message of freedom and opportunity in the Information Age, in December 2006, the Under Secretary of Defense for Policy created my office, Support to Public Diplomacy (SPD). SPD's mission is three-fold. First, we are working to create organizational change within the Office of the Under Secretary of Defense for Policy to ensure that strategic communication and information are integral to policy making, implementation, and assessment. It is important to note here that part of that cultural change means explicitly understanding that information and communication is not just what government officials say. SPD is not a public affairs office. SPD works to lessen the "say-do" gap. These efforts at cultural change are essential to SPD's second core mission: developing and coordinating key themes and messages within DOD to promote policies. In policy development and implementation, we work with DOD Public Affairs

and Joint Staff, and other Policy offices. Our third core mission is to work with other U.S. government partners, particularly the Department of State – the lead for U.S. government public diplomacy – to design and facilitate whenever possible strategic communication policies and plans to effectively advance U.S. national security.

With regard to countering ideological support to terrorism and terrorist use of the Internet, my office seeks to enhance understanding of how terrorist organizations like Al-Qaeda conduct influence campaigns, and to develop policy and strategies to counter them. As I have emphasized, increasingly these influence campaigns are being conducted via the Internet, but with immediate impact on the U.S. and partners' forces around the world.

The President's National Strategy for Combating Terrorism provides a strategic vision of the defeat of violent extremism as a threat to our way of life as a free and open society, and the creation of a global environment inhospitable to violent extremists and all who support them. The Department will continue to work with our U.S. government partners to engage the terrorist enemy in the cyber battlefield as a critical domain in our efforts to win the war of ideas and ultimately achieve the President's vision.

Thank you for the opportunity to speak with you today. I am happy to answer any questions you may have.