



FROM VIRTUAL JIHAD TO REAL JIHAD:

How Terrorists Use The Internet To Organize Attacks And How We Can Stop Them

By Henry Morgenstern

The United States has mounted an initiative to reveal how terrorist groups use the Internet. Code named Reynard, this initiative came to light when a recent report by the Office of the Director of National Intelligence was sent to Congress.





Above: Examples of Jihadi website home pages.

In the report, the initiative is described as a “seedling effort to study the emerging phenomenon of social (particularly terrorist) dynamics in virtual worlds and large-scale online games and their implications for the intelligence community”.

The global Jihad, however, is beyond seedling efforts when it comes to using the Internet to promote, organize, and execute its mission. Despite the paradox of a fundamentalist Jihad, rooted in the 7th century, efficiently using the tools of a secular 21st Century, they are doing this everyday with efficient and lethal results.

START YOUR OWN JIHAD: EVERYTHING AVAILABLE ON THE WEB, INCLUDING OUR WEB CAMS

In April 2005, US Capitol Police were busy confronting an erratic Austrian that officers feared was a suicide bomber. The force was unaware they were being filmed by men who had also documented the World Bank headquarters, the Pentagon, fuel tanks, and the George Washington Masonic memorial. These videos were uploaded to Web sites that distributed them to members around the world.

The two men, arrested in 2006 reportedly before becoming an imminent threat to the United States, may not have

accomplished an actual terror attack. But how much have they contributed to a future attack? That footage is now in the possession of Jihadi groups worldwide. Syed Haris Ahmed, one of the two men arrested, admitted that he had befriended and recruited other extremists through forums, sites and chat rooms.

WE SUPPLY THE FOOTAGE

Today, terrorists do not even need surveillance video. The proliferation of Web cams pointed at many valuable targets, made available by our airport authorities and other helpful institutions, mean that an operator in anywhere in Pakistan can instruct a comrade in Brooklyn to park his car outside a terminal at JFK and watch from Pakistan if and how authorities react. The tested methodology is just a short step from carrying out an attack using this technique.

THE JIHAD'S VIRTUAL 007

Twenty-two year old Irhabi007—a play on the word terrorist and 007—was not trained in Jihadist camps in Afghanistan, nor was he one of the Mujahadeen that learned his trade in the war against the Soviet Union in Afghanistan. But Irahbi007, a son of a Moroccan tourist official and a student of information technology, arguably did more to enable

Today, the most rudimentary Jihadists can exchange recipes for nitroglycol and thermite, as well as finance, recruit, and learn how to conduct effective Jihad against the West.

the global Jihad than even al-Qaeda leader Ayman Al Zawahiri.

As a student in Britain, he started a frightening and lethal development in the War on Terror: he used the Internet to organize and recruit for the Jihad.

In doing so, he unleashed a dangerous movement that today replaces al-Qaeda as “The Base” and relegates al-Qaeda to a strictly inspirational role. The new Jihadi networks allow for financing, planning and executing devastating attacks with relative ease.

Today, the most rudimentary Jihadists can exchange recipes for nitroglycol and thermite, as well as finance, recruit, and learn how to conduct effective Jihad against the West. Tutorials in 20 installments are downloadable and are envied by educational designers in the US as proper examples of distance learning. Even more disturbing, terrorists recently began distributing flight simulation software – making flight school obsolete. These virtual schools are disseminated with encryption software provided on Jihadi forums.

“For example, a school teacher was found on one of the forums asking for help in carrying out a mission,” says Gadi Aviran, a former EOD officer in the IDF, a veteran of Israel’s Military Intelligence Directorate (AMAN) and today the founder and President of Terrogence, the world’s leading actionable intelligence company.

Aviran says the man learned that the US President was visiting his school in the Palestine authority during a recent visit to the Middle East.

“On the forum, the teacher asked what he could do, given that he would be in close proximity to the President,” he said. “We take seriously the level of sophistication and what is being done on the Web in the name of the Jihad.”

IS THE WEST KEEPING UP WITH JIHADIS?

The western world, by most accounts, is not keeping up with the Jihadis. Instead, much attention is given to sites like Ehklaas, (www.alekhlaas.net). Though it seems an ominous site due to the extreme nature of member chats, it’s not where the serious players post. In addition, poor translations, and even poorer analysis, are giving rise to potentially deadly situations.


For example, the word for “missile” and “rocket” are the same in Arabic. There are grave consequences, however, of mistaking the intent to use a rocket when a missile is the intended weapon. A mistake such as this was recently made by a US intelligence agency based on a faulty translation provided by a private intelligence company.

As with anything in Internet time, extremism has advanced with lightning speed since 2005.

The antics of “Maximus”, a Swedish teenager of Bosnian extraction named Mirsad Bektasevic, and inspired by Irhabi007, who along with three others plotted attacks in Europe in 2005, now seem like child’s play.

When police recovered 19 kg of explosives, and video recordings claiming affiliation to al-Qaeda in Northern Europe, they also discovered Bektasevic’s contact with Irhabi007. The arrests in Sweden led to the arrest of Irhabi007 and a sentence for 10 years after pleading guilty to charges of incitement to murder and conspiracy to commit murder. The gang was also running credit card and other fraudulent businesses to finance other Jihadi sites.

On Irhabi007’s computer, police discovered the following exchange: “We



*Bomb-making recipes are available via the web for even the most rudimentary Jihadists.
Photo: BLACKHAWK!*

are 45 doctors and we are determined to undertake Jihad for Allah's sake and to take the battle inside damaged America, Allah willing."

In fact, the men referred to were the ones linked to the failed bombings at Glasgow airport and failed car bombings in London in 2007.

"Today it will be more difficult to track (the terrorists) down," says Aviran. "They are giving each other good guidelines on how to cloak their identity on the Web and how to clean up after a session. It's now a case of drawing and then connecting the dots. Doing this, we can stay ahead of our adversary in this conflict."

REAL-TIME THREAT EXAMPLE

A real time example of terrorists' use of the Internet starts with an activist from Algeria who asked online about raw ingredients needed for manufacturing an acetone-peroxide explosive. The activist wanted the resulting explosive to be used as part of a body-worn IED.

In this specific case, the Maghreb activist wanted to know if TATP (tri-acetone, tri-peroxide explosive) could be easily used in a suicide belt, specific ingredients, and commercial names the raw materials are sold under.

In less than three hours the activist received textual instructions providing him with all necessary information and a link directing him to tutorial videos with "step-by step" visual instructions for TATP "kitchen lab" manufacturing.

The understanding that these support networks may replace the more easily detectable overseas communications with global Jihad organizations, including al-Qaeda, is critical for the unveiling of local self-radicalizing cells. It is by

tracing this newer type of communication between seemingly anonymous surfers that these may be identified in time.

Reprinted courtesy of HomeLand Security Bulletin of Open Source Threats (HS-BOOST).

UNDERSTANDING TECHNO-INTELLIGENCE SIGNATURES

"It is essential that we learn to understand the traces that all activity on the Web leaves," says Aviran. "We need to associate with the entire terrorist life cycle."

Aviran gives an example of a recent incident in Florida: "Two men were fishing in the Everglades to the west of Miami with saltwater rods. A state law enforcement agent, whose job it is to enforce anti-poaching laws in the Everglades, detained the two men. Both were from countries of interest and the officer requested that they show him their car. There were no alligators in the trunk but on the back seat were maps of Miami International Airport, including arrival and departure times of airlines. The Everglades, of course, forms part of the pattern flown by flights into and out of Miami. An RPG could probably bring down an airplane there easily. The officer completely missed the signs, released the men and wrote up a report. Fortunately, someone in the agency recognized the signs and followed-up."

One of the key factors is to discern the difference between an intelligence threat and a theoretical threat. Aviran's company recently discovered on Jihadi sites a documentary on Paris sewer systems. The documentary had been in heavy distribution.

"The film was seemingly benign," he



The images above are excerpts from the original correspondence; note the time stamps on the upper bar.

says. “In the hands of a group threatening to create havoc in the French capitol, however, the information on how exactly the location of the sewage system affects the city and where it passes could be devastating if it ended up in the wrong hands. A TV show is a theoretical threat but when it shows up in forums it becomes an intelligence threat.”

Aviran suggests agencies look for the specific signatures that terrorist life-cycle activity leaves. Some signs of that activity include:

- Internet browser history
- Programs found on the suspect’s machine
- Membership in forums
- Evidence of videos about potential targets
- Evidence of financial dealings and unusual credit card activity
- Manufacture and access to components and materials for creating IED’s

Aviran’s also advises agencies to make careful collection lists before approaching the complex problem of getting into closed Jihadi forums.

Terrogeance specializes in conducting collection projects for clients like the US Department of Defense, and European and Israeli intelligence agencies.

INTERNET ACTIVITY AND TERRORIST FINANCE – SYNERGY IN CYBERSPACE

In one of the worst terrorist attacks, more than 200 people died in a 2003 bombing of a nightclub in Bali, Indonesia. They were the victims of Imam Sumadra, a militant Islamist with strong links to al-Queda.

As with other terror masterminds who have contributed to the Internet information network, Samudra wrote a jailhouse memoir instructing followers on online credit card fraud to finance terror operations.

The nexus between crime, insurance fraud, credit card fraud, and contrabanding of luxury goods to cigarettes has an inescapable online presence.

What could be done to slow this

Evidence of materials and components of IED’s are just one of the many specific signatures that terrorist life-cycle activity leaves.



repository of information on everything from Bomb-making to crimes that could finance terror and much more?

Self-regulation needs to be imposed on hosting sites. Many sites, however, are genuinely unaware of the problem. Recently in Florida, an ISP was hosting a forum on which Jihadists could download their own brand of encryption software. Notified by Law Enforcement, the site closed down the forum. There are also many barriers to controlling the Internet. As a society, we have yet to make unifying decisions about Internet issues, including spam, and online criminal activity and fraud protection. A consensus on what and who constitutes a threat to citizens in an Internet democracy may be far away.

THE NEW HOME OF TERROR – THE INTERNET

The expert use of the Internet is evidenced by propaganda issued by groups that espouse the Jihadi ideology. A recent propaganda film released by such groups in Iraq uses a real US soldier, “Lees Life of Lies and details about his life (based on stolen documents), to construct a very impressive hour long, high-value production movie that purports to show US soldiers criticizing the war in Iraq. When we show these documentaries at SSI training sessions, most viewers do not believe them to be fake. It’s the kind of propaganda that would impress Leni Riefenshtal.

Our challenge is to keep up with the Flinstones. Failure to do so will have tragic consequences for the War on Terror. We need a concerted national effort – similar to the one made during the Cold War – to train pro-Western Arabic speakers to help decipher terrorist cyber codes. Without that, we are constantly reacting to the advances of the Jihadis.

Michael Doran, a Near East scholar and terrorism expert at Princeton University says this: “When we say al-Qaeda is a global ideology, this is where it exists—on the Internet.”

Indeed, we need to quickly become Internet savvy to counter this impending threat. ●

ABOUT THE AUTHOR

Henry Morgenstern is the President of Security Solutions International. He has been published in scores of Law Enforcement publications, counter-terrorism publications and print and electronic media. In addition, he has appeared on NBC, CBS and Fox as a commentator on terrorism issues.

INTERNET JIHAD: WHERE IS IT HAPPENING?

<http://www.m3ark.com/forum/>

A partially closed forum supportive of global jihad. A vital participant in the distribution of propaganda and weaponry / explosives manufacturing material.

<http://hanein.info/vb>

A forum supportive of global jihad and of regional insurgent groups. Prominent distributor of jihadi films, including self-produced multimedia.

<http://www.muslim.net/vb/>

A forum supportive of global jihad and of regional insurgent groups. One of the leading platforms for the distribution of Jihadi multimedia material.

<http://www.paldf.net/forum/>

A forum supportive of the Palestinian

resistance. Prominent distributor of jihadi multimedia and propaganda produced by Palestinian insurgent groups.

<http://www.military.ir/>

A general forum in the Farsi language. Members of the forum discuss military and political subjects concerning Iran.

<http://www.cecenya.net/>

A website in the Turkish language supportive of the Chechen resistance. Distributor of jihadi multimedia and propaganda concerning Chechnya.

<http://www.velfecr.com/>

A website in the Turkish language supportive of the Palestinian resistance and of the Lebanese insurgent group Hezbollah. Publishes news flashes, articles and jihadi multimedia. ●