

7 January 2009

By: Lucian Constantin, Web News Editor



Cyberwar between  
Islamic and Israeli  
hackers  
Cyberwar Wiki

## [The Gaza Strip Cyberwar](#)

*Numerous computer hacking incidents accompany the ongoing armed conflict*

Cyberwar is not just a distant concept anymore. Every recent armed or political conflict has been accompanied or followed by Internet-based attacks spreading propaganda or targeting vital infrastructure. The Israel - Hamas conflict in Gaza makes no exception to this rule, and has attracted what looks like a massive wave of hacking incidents affecting both sides.

Many groups, even from the western countries, expressed their disapproval regarding the Israeli offensive in the Gaza Strip, but nothing compares to the anger of the Hamas sympathizers from the Arab world. Hacking crews from Morocco, Lebanon, Turkey, Iran, Egypt, and other middle-eastern countries united their forces and launched hundreds of attacks targeting Israeli websites.

Security researchers estimate that around 10,000 individual web pages hosted on the co.il domain space have been defaced by these hacking groups, which are using underground forums to coordinate their attacks. Many of the defacements have been posted on tracking websites such as the Arabic Mirror.

A more serious incident was caused by a Morocco-based Islamic hacking group calling themselves "TEAM-Evil," who obtained unauthorized access to the database of the Domain The Net Technologies registrar by using stolen credentials. This gave them the ability to alter the name servers of several important Israeli websites. The YnetNews.com domain name, belonging to a popular Israeli online news service, was amongst the ones affected, the hackers redirecting its traffic to a page displaying violent images and messages.

"The fact that hackers were able to breach DomainTheNet, by allegedly using valid client passwords, is highly disturbing," Ynet's Editor in Chief, Jon Feder, [commented](#). "Ynet is looking into all aspects of the incident, be they technical, procedural, or legal vis-&agrave;-vis the domain registration service, and the matter will be dealt with without delay," he added.

Israeli hackers did not wait long to retaliate, and launched their own counter-offensive, culminating with the hacking of Hamas' Al-Aqsa television network by the Israeli Defense Forces (IDF). The station appears to have been considered an important target ever since the beginning of the conflict, considering that its studios have begun to be bombed as early as the second day of the air offensive.

Al-Aqsa attracted the hate of many Israelis in 2007, when they aired an anti-semitic cartoon. Reports claim that the broadcasts of both the Al-Aqsa TV and radio stations were disrupted on Saturday by an image and/or sound of a ringing phone that remained unanswered, followed by an audio message in Arabic that said, "Hamas leaders are hiding, and they are leaving you on the front line."

According to [Wired](#), things escalated on Sunday, when the TV station's broadcast was hijacked again in order to transmit more propaganda. This time around, an animation clip of Hamas leaders being gunned down was aired, accompanied by a warning that read "Time is running out."

Similar cyber-attacks were launched by Islamic hackers in 2006, against websites in Denmark and U.S., after a Danish newspaper published a cartoon portraying the prophet Mohamed. Russian hackers are also famous for directing such attacks against [Lithuania](#), Estonia, or [Georgia](#). The U.S. military recently [banned](#) the use of portable media devices on its networks, in order to contain a massive computer virus infection, which some claim was [specifically designed](#) by unknown hackers to steal secret information. Meanwhile, South Korea is constantly [pointing the finger](#) at its communist cousins from the North for using computer spyware in order to steal its military secrets.