Is the Internet a New Space for Waging War?
The Case of the Islamic Fundamentalists and their Opponents

Uros Svete

I. Introduction

Although the early definitions of information warfare\(^2\) go back to the 1990s or even earlier in 20\(^{th}\) century, many authors like Caforio\(^3\) have characterised the NATO air campaign and following conflict against the Federal Republic of Yugoslavia in 1999 as probably the first war on the internet; cyberspace was not just a significant sphere of presenting a conflict, but had become a place for waging a war in the sense of causing physical information damage to the opposite side. The growing importance of cyberspace at this time was indicated by attacks against NATO mail and web servers, by hackers’ international cooperation and political engagement (better known as hacktivism), by the CIA’s alleged attempts of hacking President Slobodan Milošević’s bank accounts, as well as by the abundance of web sites created by opposing sides and the importance of this kind of information for journalism (media coverage). In contrast to the Kosovo war, which occurred between countries with high levels of development and information diffusion (Yugoslavia included), the recent conflicts between Islamic fundamentalists and their opponents takes place in countries such as Iraq, Afghanistan,

---

1 Uros Svete is teaching assistant at the Defense Studies Division of the Faculty of Social Sciences of the University of Ljubljana. This paper was presented at the Second Annual Conference on Human Security, Terrorism and Organized Crime in the Western Balkan Region, organized by the HUMSEC project in Sarajevo, 4-6 October 2007.
2 Information warfare is the use and management of information in pursuit of a competitive advantage over an opponent. Information warfare may involve collection of tactical information, assurance that one’s own information is valid, spreading propaganda or disinformation among the enemy, undermining the quality of opposing force information and denial of information-collection opportunities to opposing forces. Information warfare has to be strictly separated from information-based warfare. Information was always significant and decisive part of the warfare, but with the informatization (I refer to the process primarily by which information technologies, such as the World Wide Web and other communication technologies, have transformed economic and social relations) of practically all social spheres, the possibilities have multiplied, and the information sphere has not just become a crucial but also the only space, where the war is being waged. Information warfare has psychological as well as (physical) destructive dimensions, which is an important difference between information and psychological operations as well between information warfare and information-based warfare.
Chechnya, Lebanon, Somalia etc, that can be characterized as economically and technologically underdeveloped. They belong to the group of so-called “technology followers”. Therefore, internet access, technological devices and knowledge are not just a privilege of rich states and societies anymore and they are able to significantly influence conflicts that take place in developing countries. As Peter Lamborn Wilson pointed out in 1995, the net has suddenly turned into a space in which power is dispersed rather than centralized. Accordingly, it was just a matter of time before the internet communication capabilities will also be used for destructive and harmful purposes by particular asymmetric, terrorist or other radical groups from all over the world. In this sense, the use of the internet by Islamic fundamentalists presents a kind of precedent, because for the first time (with exception of Chiapas guerrilla warriors), the Internet has become a very strong weapon in the hands of societies where the technology sector is principally less developed, but where there are a large number of very skilled and educated individuals. The internet originated as a military space designed in order to avoid the psychical disruption involved in the event of atomic warfare. The big paradox is that 40 years later the Islamic fundamentalists sometimes use the American advantage in their own favour. The one-time Western advantage in information dominance has become today’s vulnerability.

The next development in today’s internet activities has already taken place in the conflicts between Islamic fundamentalists and their opponents. The role of the individual has become increasingly more important, especially in comparison with national states and supranational organisations such NATO or the UN. F. Pierantoni and M. Pierantoni defined cyberspace as a space in which the role of official organisations like UN and NATO will be increasingly marginalized whereas the virtual connection among people at any level, and not only those involved in the intelligence sector, will become increasingly important. The empirical cases considered in this paper clearly confirm this thesis. Internet wars are carried out more often between individual hackers or groups that practically, albeit informally, represent some of the sides involved in the conflicts. Although the hackers’ activities comply with state interests, hackers very rarely belong to official institutions especially in the West, not taking into account hacker intelligence (with the exception of the well-known special military units comprised of hackers that have been established by the People’s Liberation Army in China). We may even claim that wars are moving increasingly into the domain of civil society while the state has been losing its monopoly for waging war gradually.

However, we should remain aware of the fact that the state also maintains its interests in cyberspace. There have been many initiatives at the state or even the supranational level regarding the prevention or reduction of the internet activities of terrorist or fundamentalist organisations as well as those of other malicious individuals. However, recent incidents such as when German government information systems were attacked by Chinese (military) hackers, the failure of the Carnivore project or the use of controversial Bundestrojaner software indicate that state institutions are losing control over the internet, especially when they attempt to repress electronic communication. It seems that individuals skilled in technology - hackers working for different types of non-state organisations - maintain the upper hand against technicians employed in national (security) institutions.

---

5 Caforio, Giuseppe, *Kosovo: War on the Internet*, at p.95.
II. Information Activities of Islamic Fundamentalists

Perhaps the most intensive media covered conflict is the war in Iraq, where scenes of extreme violence are recorded by mobile phones and digital cameras and transmitted over the internet nearly every day. These images show, for example, beheadings and the detonation of improvised explosive devices. On the other hand, images that should not be forgotten, such as the execution of former Iraqi dictator Saddam Hussein and the pictures from the Abu Ghraib prison have also been transmitted via the internet. Media have been used very efficiently, especially in information warfare and psychological operations (sometimes better known as propaganda, if we use the old term. Psychological Operations (PSYOP, PSYOPS) are techniques used by military and police forces to influence the emotions, motives, objective reasoning and behaviour of a target audience. Target audiences can include governments, organizations, groups and individuals, and these techniques are used in order to induce confessions, or to reinforce attitudes and behaviour favourable to the originator's objectives. Psychological warfare/operations are always perceived as an additional war technique; however, fundamentalists claim, in regard to the information warfare, that in the near future war will be waged just within the information space). Iraqi Islamic fundamentalist groups as well terrorist organisations have used information technology and digital media to influence the domestic public (in order to gain its support) as well as the international (especially Western) or global public. Islamic groups and certain media (including the Arab information services Al Jazeera and Al Arabiya) are very skilled in using the advantages of information-communication and satellite technologies to present violence against kidnapped civilians and soldiers in order to influence, above all, the Western public. Their sympathisers upload videotaped wills of suicide bombers, post claims of responsibility for attacks and write monthly online magazine articles on topics such as urban warfare, how to choose a target or how to raise a child to be a "martyr".

Consequently, the use of the internet plays a significant role in the logistic, operational and communication network of terrorist organizations. Terrorists use the internet not only as a means to communicate and spread propaganda, but also to radicalize, recruit and train members and supporters all over the world. The internet is also employed as a means to spread instructions on how to execute concrete offences and to transfer information, as well as for terrorist financing purposes. So-called terror manuals provide instructions on how to produce weapons, how to launch effective attacks, how to take hostages and how to build bombs, among other things. In the face of the global availability of the internet, this is especially worrying. These two web portals are examples of such activities: the Kavkazcenter.com - http://www.kavkazcenter.com and Islambosna.ba - http://www.islambosna.ba. Both of these sites indicate terrorist awareness for using local languages, dispersal web pages and different internet services. Without them, the global effects as well as the goals of the (Pan)Islamic movement could never be achieved.

But it is also remarkable how Islamists have gotten savvier in their use of the internet. When Iraqi insurgent Abu Mussab al-Zarqawi and his group posted the video of the execution of Nicholas Berg in 2004, an American contractor working in Iraq, the web site where it was shown was quickly overwhelmed with traffic. Today jihadis post evidence of their operations
on dozens of sites\(^6\) (some of them already mentioned) and coordinate their operations on secret e-mail lists, password-protected web sites and audio chat services like PalTalk, which don’t leave behind a printed record. The level of sophistication of these groups has become unbelievable.

Figure 1: The Web Portal [http://www.islambosna.ba/](http://www.islambosna.ba/)

---

III. Preventing Cyber Activities – Is It Possible at All?

A. Nongovernmental Institutions

However, when conducting an analysis of the Islamist information and communication activities, the opposite side, the opponents of the Islamic fundamentalists, must also be taken into account. These are numerous and heterogenic, from particular pro-Israeli or pro-American civil society groups or associations\(^7\) (Internet Haganah- [http://www.haganah.us/haganah/internet.html](http://www.haganah.us/haganah/internet.html)), Jihad Watch- [http://www.jihadwatch.org/](http://www.jihadwatch.org/) and [http://siteinstitute.org/](http://siteinstitute.org/) to some national states or even supranational organisations such the European Union. But regardless of this disunity, the awareness for monitoring and preventing Islamic fundamentalist web pages and activities has been spreading very quickly during the last months.

\(^7\) More or less supported by some national authorities.
Firstly, we have to mention Internet Haganah\(^8\) a "global intelligence network dedicated to confronting internet activities by Islamists and their supporters, enablers and apologists." Internet Haganah is also an activist organization which attempts to convince businesses not to provide web-based services to such groups, and collects intelligence to store and pass on to government organizations. It was formed by Aaron Weisburd in 2002, and became part of a collection of private anti-terrorist web monitoring companies that also includes the "Terrorism Research Center", the "Search for International Terrorist Entities Institute", and the "North-east Intelligence Network". Weisburd is the only full time employee of Internet Haganah, which is run primarily from his home office with the help of many online associates. There are two main parts to Internet Haganah:

- A small, global band of researchers, consultants, analysts and translators who associate and collaborate with each other as necessitated by a common desire to do more than just watch Islamists as they use the internet. Internet Haganah shares an understanding that a jihad, or holy war, has been declared against the West, and that jihadists need to be met on whatever field of battle they may appear.

- The parent organization The Society for Internet Research operates this web site [http://www.haganah.org.il/](http://www.haganah.org.il/), which has approximately 30,000 visitors per month.

The organization claims to have taken down approximately 730 Jihad sites. To target web sites perceived as threats, the organization relies upon its web community to find jihadists, and use a free "who is" service to determine if a US based server hosts them. If so, as in the case of mawusat.com and its host Go Daddy, Internet Haganah operatives express concern about the nature of the site and ask the host to remove it. If this does not work and if the site concerns the US State Department's list of Foreign Terrorist Organizations, or the US Treasury's Office of Foreign Asset Control's list of Specially Designated Nationals and Blocked Persons, Internet Haganah contacts the Banks and Financiers of the host, who could face serious penalties for engaging in unreported transactions with the suspect web site. If all else fails, the media may be contacted.

---

\(^8\) Haganah is a Hebrew word meaning "defence". Haganah is also the name of a militia originally formed to defend Jewish settlers in what was then British occupied Palestine, and which evolved into what is now the Israel Defence Forces.
However, as the defence become more elaborate, so does the offence. In the case of Go-Daddy.com and mawusat.com, the site was attacked, but reappeared on a different server within a week.

The second example is The Search for International Terrorist Entities (SITE) Institute (http://siteinstitute.org/), a non-profit organization which tracks the online activity of terrorist organizations. The SITE Institute was founded in 2004 by Rita Katz (Iraqi born Jewish) and Josh Devon. What especially needs to be mentioned are the changes within the intelligence community of the USA, caused by such “civil society and non-profit organisations”. Traditionally, intelligence has been filtered through government agencies, such as the CIA and the NSA, which gather raw data and analyze it, and the government decides who sees the product of their work and when. Katz has made it her business to upset that monopoly. She and her researchers mine online sources for intelligence, which her staff translates and sends out by e-mail to a list of about a hundred subscribers. Katz’s client list includes people in the government who are presumably frustrated by how long it takes to get information through official channels. Among the clients are also people in corporate security and in the media who rarely get much useful material from the CIA. She has worked with prosecutors on more than a dozen terrorism investigations, and many American officers in Iraq rely on Katz’s e-mails to, for example, brief their troops on the designs for explosives that are passed around terrorist web sites.  

The last examples of civil-based information war are Islamic web pages, which were and still are targets of pro-Western hackers. During the first phase of Iraqi war in 2002, numerous Iraqi official as well as Islamic web pages had been changed or even removed from cyberspace: this was just one way how to prove technological superiority over opponents.

---

B. The Reaction of the State- Some Examples from the USA and Germany

Before the September 11, 2001 attacks, the official counterterrorism agencies in Western countries paid relatively little attention to the presence of Islamists online; however, this has changed over the past few years largely due to changes in the way terror networks operate, as previously described. To aid understanding, we will present some of the initiatives from the United States, Germany and the European Union. First, such technical measure is the Carnivore system implemented by the Federal Bureau of Investigation. The Carnivore system is analogous to wiretapping, except that in this case, e-mail and other communications are being tapped instead of telephone conversations. Carnivore was essentially a customizable packet "sniffer" that could monitor all of a target user's Internet traffic. It is a form of policeware.  

US government officials have neither confirmed nor denied much about the physical or logical workings of Carnivore, but there are some basic facts that are generally agreed upon. The Carnivore system itself is simply a Windows workstation with packet-sniffing software and a removable disk drive. This computer must be physically installed at an Internet Service Provider (ISP) or other location where it can "sniff" traffic on a LAN segment to look for email messages in transit. The technology itself is not highly advanced - using a standard packet sniffer and some fairly straightforward filtering (such as a Perl script), one could easily dupli-

---

10 Policeware is software designed to police citizens by monitoring discussion and interaction of its citizens.
cate this functionality. Getting the cooperation of the ISPs or the owner of the LAN onto which Carnivore is to be placed can either be voluntary or by court order. However, once a system is in place, it is allegedly not allowed to simply capture every email that passes through the system - by existing US law, publicly acknowledged US Government personnel are required to get a warrant or court order naming specific people or email addresses that may be monitored. When an email passes through that matches the filtering criteria mandated by the warrant, the message is logged along with information on the date, time, origin and destination. This logging is believed to be relayed in real time to the FBI but the details are not currently known. All other traffic would presumably be dropped without logging or capture.

There is much speculation and concern regarding the implementation, usage and possible abuses of Carnivore. Free speech advocates and others interested in civil rights are concerned about the potential for misuse and infringements on individual's right to privacy. On the other hand, there has been a doubt of Carnivore capability. Analogies have been drawn between Carnivore and Echelon, which was established primarily for surveillance in intelligence data gathering during the Cold War. Carnivore should intercept all electronic digital communications. But when Echelon was growing up for the centuries, Carnivore ought to become operative in very short time and with technology that foresaw the cooperation of the ISPs. It is completely understandable that Carnivore failed to fulfill these demands.

The next example is Magic Lantern, a keystroke logging software developed by the Federal Bureau of Investigation. Magic Lantern was first reported in a column by Bob Sullivan of MSNBC on 20 November 2001. Unlike previous keystroke logger programs used by the FBI, Magic Lantern can reportedly be installed remotely, via an e-mail attachment or "by exploiting common operating system vulnerabilities". It has been variously described as a virus and a Trojan horse. It is not known how the program might store or communicate the recorded keystrokes. Like Carnivore, the existence of Magic Lantern in the public sphere has also been disputed. FBI spokesmen confirmed soon after the existence of a program, but denied that it had been deployed, and they declined to comment further.

The public disclosure of the existence of Magic Lantern sparked a debate as to whether anti-virus companies could, or should, detect the FBI's keystroke logger. Birdis reported that at least some anti-virus companies, including Network Associates (maker of McAfee anti-virus products) had contacted the FBI following the press reports about Magic Lantern to ensure its anti-virus software would not detect the program. Network Associates issued a statement denying this kind of cooperation with US legal authorities within a week, fuelling speculation as to which anti-virus products might or might not be capable of detecting government trojans. The same story played out with the so called "Bundestrojaner", a trojan produced by the German Ministry of Interior. The program, which should control terrorist, fundamentalist

---

13 German government plods are asking to be allowed to email trojan horse spyware to terrorist suspects in order to surreptitiously monitor their internet use and inspect their computer hard drives remotely. Interior Minister Wolfgang Schäuble proposes to include this authorisation in a security law now under consideration in the German parliament. The spyware would be hidden in emails appearing to have been sent from other, seemingly innocuous government agencies such as the Finance Ministry or Youth Services Office. The measure is being proposed because Germany's Federal Court of Justice in February rejected prosecutors' earlier plans to search suspects' computers remotely over the internet. Prosecutors had argued that such invasive remote investigation
and criminal activities in Germany, has become a matter of conflict between government, civil society and anti-virus software producers. As it seems at the moment, this supervision is being carried out under the supervision of the Federal Interior Minister, who is, in fact, an enthusiastic supporter of American homeland security and the anti-terror strategy concept. While the German case exposes the awareness of privacy protection, the same story in Austria resulted in a completely different outcome. It seems just a matter of time until Trojans and other supervising software will become operative instruments in the hands of federal investigation and prosecution authorities.

The last organisation that joined this “cyber preventing” strategy is the European Union. The EU wants to strengthen its monitoring of militant Islamic web sites, and says that the internet plays a major role in the operations and communication networks of terrorist organisations. EU ambassadors gathering for their weekly meeting in Brussels on 30th May 2007 decided that a newly established online police portal "needs to be further strengthened" to combat terrorism. The high-security portal - named "Check the Web" - allows the 27 EU states to pool data on Islamist propaganda and internet chatter at the European Police Office (Europol) in The Hague. The EU member states are allowed to share their responsibilities in checking the web, and they are also allowed to share information that could lead towards greater synergy and save energy at the same time. The site is only accessible to a maximum of five experts from each EU state.

IV. Conclusion

The internet, along with other modern media, has dramatically changed our perception of conflict, and also undoubtedly become a new space for waging and reflecting on conflict. At recent stage we still could not find physical implications of cyberwar, but technological base for such activities exists without any doubt. Critical infrastructure, based on information-communication technology, could be affected also physically, although the cost-benefit analysis for today’s terrorist, it is much easier just to spread propaganda and using internet interactivity capabilities for communication and information exchange. Of course we should be aware of the internet’s limitations. A problem that has to be considered is that of propaganda research when we are talking about internet. User anonymity does not allow us to check the influence of the internet in society in a precise or methodically correct way. The second problem regarding propaganda spreading in the internet is its interactivity. For some reason, revolutionary advantage in the case of propaganda is much more of a hindrance than a possibility. For the use of traditional media, the user’s active participation is not necessary; the internet,

should be permitted because it was analogous to telephone surveillance or other forms of electronic eavesdropping, but the German court didn't buy that, prohibiting the practice because there was no law that specifically permitted such monitoring. Do German gumshoes believe that real terrorists won't have capable antivirus and antispyware software installed? One can imagine they'll probably be immune anyway, because they're likely already running OS/X, BSD or Linux (Orion, 2007).


15 Meanwhile the empirical data of the internet users could not be comparable with the television, radio and newspapers audience, we also have to consider internet importance for journalists working for traditional media (See Figure 2). The Internet is becoming one of the most important news sources for such traditional media, what increases its at the first sight limited social implications. So the fact the smaller number of the internet users comparing with traditional media, has to be relativized.
on the other hand, demands some kind of basic computer and information knowledge. Also, the information gleaned from the internet is accessed by users only to a very limited extent. Because every coin has two sides, analysing internet suitability for the spread of propaganda, we have to mention censorship is very hard to carry out. As it was shown in this paper, there have been numerous attempts by civil society as well by national authorities to control and supervise internet use, but the effectiveness is more or less doubtful.

When the cases presented in our analysis confirm the presumption that recent cyberwar particularly presents virtual or symbolic parts of conflicts, in the age of globalisation the internet has become one of the basic tools ensuring transnational terrorist networks in the real world. We could even risk a thesis: without the internet, transnational Panislamic terrorist groups could not achieve their political, cultural and strategic objectives, at least not in such short amounts of time. Consequently, this is one of the main reasons why state institutions or even civil society groups are trying to prevent such Islamist information activities. The crucial question is how effective these attempts could be, and last but not least what kind of effects they supposed to have in frame of human rights and privacy protection. Therefore, a dilemma between national and human security concept compatibility is reasonable. The question is if the internet is becoming a tool in hands of national security for combating terrorism or a tool for threatening human security interests at the same time. The examples of internet monitoring attempts in USA, EU, Germany and other countries show how thin the line between national and human security interests is. Of course, the citizens are interested in safety and security, but at the same time they are not always prepared to sacrifice their individual rights in the name of privacy protection.

When the first dilemma refers to security interests and instruments ensuring it, the second very important issue discusses the role of traditional national and supranational security actors in the information age. We could agree with a thesis that national and supranational authorities are losing their influence and power particularly in comparison with individual and non state-internet users like terrorist, extremist and fundamentalist organisations. The lack of international accepted regulations and the technological accessibility like free code exchange give unpredictable power to the already marginal social groups. So, the internet, created for national security interests, is becoming a tool by which national as well human security interests have become threatened. So how can this problem be solved? Some suggest that the internet has to be shared when one closed network would be designed just for national authorities (Internet 2), the rest ought to stay open for all other users. I am not sure if such suggestions are heading in the right direction, because the relationship between the internet and society that uses it is dialectical. The internet, while mirroring social development, also generates social change, a fact which should never be forgotten.

16 Svete, Uroš, The role of Internet in the War against Terrorism - Threatening Privacy or an Ensuring Mechanism (national) Security - the Slovene Perspective, in Politics in Central Europe (Volume 2, Number 2), Winter 2006/2007, pp. 71-82.
References


Orion, Egan, Germany wants to email spyware to terror suspects. Could this daft plan really work?, 2007. Available online at: http://www.theinquirer.net/?article=42071


Svete, Uroš, Varnost v informacijski družbi (Security in the information society), Ljubljana Fakulteta za družbene vede (Faculty of Social Sciences), 2005.


Woo, Christopher and Miranda So, The case for Magic Lantern: September 11 highlights the need for increased surveillance in Harvard Journal of Law & Technology (Volume 15, Number 2), Spring 2002, pp. 521-538.

The HUMSEC project is supported by the European Commission under the Sixth Framework Programme “Integrating and Strengthening the European Research Area”.

12