

# Preface

The Internet, or the ARPANET in its original name, was a remarkable idea. The Net was designed in the late 60's by US ARPA (Advanced Research Projects Agency) to connect distant computers to each other. This was a critical need at a time when each computer was a precious resource of computing power, which, if connected, could be shared among several groups of researchers at multiple physical sites. Like in many other engineering projects, the ARPANET designers could hardly foresee all future uses of their new infrastructure. Probably, the vision of Internet cafes and airport passengers checking email on their laptops was far beyond their imagination. The fact is that long before computers became affordable and "personal", a major part of the cyberspace traffic shifted from connecting computers engaged in some computationally intensive tasks to connecting the users of those computers — the people. Thus, a special ARPA survey has found in 1973 that as much as three-quarters of all net traffic was nothing more sophisticated than electronic email<sup>1</sup>. Disregarding what ARPA personnel could think or do about it, the cyberspace was moving on its own, hardly controllable way.

Today, in the middle of the first decade of the 21<sup>st</sup> century, the Internet connects millions of computers worldwide and its traffic originates from unaccounted number of computing applications. The cyberspace has become a major communication medium, where virtually any kind of content can be transferred instantly and reliably between individual users and entire corporations that may be located in totally different corners of the planet. The invention of the World Wide Web (WWW) in the early nineties had a particularly significant effect on the cyberspace evolution. On WWW, the

---

<sup>1</sup>J. Naughton, *A Brief History of the Future: the Origins of the Internet*, Phoenix, 2000, p. 141

person posting the information to a web site, the web site itself (i.e. the web server hosting it), and the visitors of that site do not have to be at any geographical proximity to each other or conform to the same law system. The Net users even do not have to disclose their real identity, not talking about many ways to "spoof" web site names, email addresses, etc.

The continuous and global war on terror, further intensified after the tragic events of September 11, 2001 in the US and more recent acts of violence in Indonesia, Spain, and other countries, does not seem to be directly relevant to the cyberspace revolution. After all, as believed by many, the most dangerous terrorists are hiding in caves or refugee camps with very limited communication capabilities, most of them never use a computer in their life, and even if they do, computer is not a weapon – one cannot kill a massive number of people with a click of a computer mouse! To examine what terrorists really do or don't do on the web, the editors of this volume have organized in April 2004, at Tel-Aviv University, Israel a one-day workshop entitled "Fighting Terror in Cyberspace". The workshop, briefly advertised in the local media, attracted a surprisingly large number of about 200 researchers and professionals, who probably considered the "terror in cyberspace" as something more than just a random combination of unrelated, though popular, terms. The highlights of the talks by workshop speakers, most of whom also contributed the chapters to this volume, were novel and disturbing.

The truth is that the Cyberspace is an ideal environment for international terrorist groups<sup>2</sup> willing to communicate with each other at maximum security and minimal cost. Abe Wagner (Chapter 1) has identified the following four areas of terrorist use (and abuse) of the Internet: covert communications, intelligence gathering on potential targets, propaganda dissemination, and attacks on the Internet itself and the critical infrastructures connected to it. All these activities can be safely conducted under the anonymity cover provided to the web users by Internet cafes, wireless access points, and alias email accounts. Public availability of advanced encryption techniques, including steganography, adds one more powerful level of security to those who have something to hide from the law enforcement authorities. The cyberspace is also a rich source of detailed information on chemical, biological, and even nuclear warfare.

The role of the cyberspace in the global jihad waged by the radical Is-

---

<sup>2</sup>The terrorist organizations mentioned by the authors of this book are included in the list of U.S.-Designated Foreign Terrorist Organizations, which is updated periodically by the U.S. Department of State, Office of Counterterrorism.

Islamic terror organizations is analyzed by Shaul Shay in Chapter 2. While disseminating a deep hatred to all attributes of the Western culture, the Al-Qaeda organization has already proven its efficiency in exploiting the Western technology for its own needs. The Internet, as an infrastructure designed by the US Department of Defense, is not an exception: Al-Qaeda operatives are widely using it for exchanging encoded messages that contain seemingly innocent content and gaining background information prior to terrorist attacks. The brutal footages of hostage killings by Iraqi insurgents have recently demonstrated the crucial role of the cyberspace as a battlefield in psychological warfare, which is a core activity of any terrorist organization.

It is time to ask ourselves a legitimate question: are we going to lose this information battle in the medium created by the best of our own minds? Are we going to lose the cyberspace to the stateless, yet smart and ruthless, enemy? The information battles of the 21<sup>st</sup> century can be fought and won by no other means but information technology. Chapter 3 by Mark Last explains the potential contribution of the state-of-the-art data mining techniques to the central tasks of cyber security and cyber intelligence. With data mining tools, the counter-terrorist agencies can discover hidden links between seemingly unrelated individuals, effectively monitor dynamic content of terrorist web sites, identify changes and trends in web documents posted by terrorist organizations, and detect dangerous anomalies in the behavior of mission-critical software systems that may be subject to cyber attacks.

Chapter 4 by Bracha Shapira presents a content-based model for monitoring web users that may be involved in terrorist activities while visiting numerous web sites maintained by various terrorist organizations. The model feasibility stems from the well-known fact that users' surfing interests tend to conform to relatively stable patterns. Different groups of users usually differ in the content of web sites they normally visit. The normal profile of a group can be induced by the data mining methodology of cluster analysis and then used to detect any suspicious deviation from the norm.

Chapter 5 by Yuval Elovici shows how the model of Chapter 4 is implemented as the core methodology of the Terrorist Detection System (TDS), which is aimed at tracking down suspects that access terrorist-related content on the web. The initial experiments with the system, based on the web content log of a group of university students, have shown significant improvement vs. a state-of-the-art anomaly detection system, which used only Operating System commands issued by the users.

A further improvement in anomaly detection performance when analyzing web content is reached in Chapter 6 (by Menahem Friedman, Moti Schneider, and Abraham Kandel) via novel clustering techniques based on fuzzy logic. This is not a surprising result, since fuzzy logic and fuzzy set theory are known to be particularly efficient for modeling approximate concepts such as similarity of web documents.

In Chapter 7 of this volume, Yehuda Shaffer describes one of the most important aspects in the global war on terror – detecting and stopping the terror financing. All known techniques of money laundering developed by criminal networks are implemented, and sometimes enhanced by terrorist organizations. This is a truly information combat, since most suspicious funds are transferred electronically. As indicated by Shaffer, a growing part of financial information is transferred via the Internet.

Though English is still the leading language of the Internet, web documents in foreign languages are important sources of information on international terrorist groups. Along with developing new automated translation tools, the research community is currently focused on direct detection, extraction, and summarization of documents in multiple languages. In Chapter 8, Alex Markov and Mark Last describe a novel, graph-based methodology for cross-lingual classification of web documents. The methodology has reached high accuracy rates on a collection of authentic web documents in Arabic.

The goal of this book is to present an up-to-date survey of threats, challenges, and tools in cyber warfare on terror. As information technology continues to move forward and become more affordable for people around the world, the threats of cyber terror in all its forms can be expected to grow, along with our capability to develop more sophisticated tools than can detect, analyze, and prevent these malicious activities. We have to face the reality: there *are* terrorists in cyber space, or "cyber caves" if you wish.

## Acknowledgments

We thank all the contributing authors who, despite their busy schedule, have responded enthusiastically to our invitation by giving a presentation at the Fighting Terror in Cyberspace Workshop and then submitting a chapter to this volume. We would also like to thank Marina Litvak who has done the final formatting of the book. The preparation of this volume was partially supported by the Fulbright Foundation that has granted Prof.

Kandel the Fulbright Research Award at Tel-Aviv University, Faculty of Engineering during the academic year 2003-2004.

*Mark Last and Abraham Kandel June 2005*