

Jazeera Space Channel TV Station
Attn: Suleiman Al Khateeb
P.O. Box 231234
Doha
Qatar

Via e-mail *suleiman@omnix.com*

Saturday, April 5, 2003

PROPOSAL FOR HOSTING AL JAZEERA WEBSITES

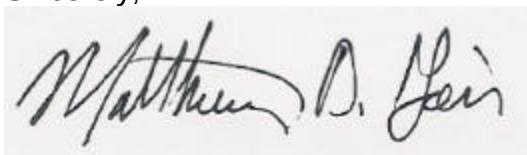
Dear Suleiman,

Thank you for your interest in Melior, Inc. and the opportunity to introduce to you our unique distributed Denial-of-Service defense tool iSecure, by which we also offer hosting solutions, which is safe against dDoS attacks, and also fully cloaked, so any hacker cannot determine the configuration of servers and other network devices.

In the following proposal we offer solutions for immediate, short-, and long-term solutions, which we hope you will find to be the solution to keep Al Jazeera's websites permanently on the Internet without any interruptions.

We are readily available to work with you at any time to migrate your sites.

Sincerely,



Matt Gair
Co-Founder and Vice President Strategic Business Development

Melior, Inc.

United States of America – Europe – Asia
US HQ: 1501 Beaumont Street, Dallas, Texas 75215
www.MeliorInc.com – www.dDoS.com – www.BGP4.com – www.Secure.SH
Tel +01-214-421-5975 Fax +01-214-421-5951

PROPOSAL FOR HOSTING “AL JAZEERA” WEBSITES

1. Current Issues
2. About Melior, Inc. - Background
3. About Melior's iSecure CyberWarfare Defense Product
 - a. Product Description
 - b. Functionality: distributed Denial-of-Service Defense
 - c. Functionality: Infrastructure Cloaking
 - d. Demonstration & Proof
4. About Melior's Hosting Solutions
 - a. Reliability
 - b. Availability
 - c. Security
 - d. Secure Management by Customer
5. Proposed Solution: Immediately (Hosting in current Melior facility)
6. Proposed Solution: Short-Term (Hosting in carrier-neutral facility)
7. Proposed Solution: Long-Term (Hosting in Qatar)
8. Other Issues:
 - a. Why does Melior offer hosting services to Al Jazeera?
 - b. No US Export Restrictions
 - c. Political Considerations
 - d. 7x24 Support Available via US (Dallas) or India (New Dehli)
9. Next Steps

1. Current Issues

Over the last few weeks the Al Jazeera websites have been continuously attacked, foremost the site “english.aljazeera.net”, resulting in unavailability. The website has been moved several times, to France and last to the distributed infrastructure provided by Akamai, which could also not provide the desired reliability, as it could not sustain the ongoing attacks.

At the time this proposal is written, the site “english.aljazeera.net” is only available with the homepage from cache, subsequent web pages remain unavailable. Al Jazeera is unable to share its content on the Internet in the English language version.

At this time, the search term “Al Jazeera” is the most popular on the Internet, ranked #1 on the Lycos statistics page at <http://50.lycos.com>, which is likely a result of the lack of availability of the website to visitors.

News media have widely reported distributed Denial-of-Service attacks as the cause of the unavailability, and reported that Akamai has now declined further service. As a reputable, high-end hosting provider this leaves few choices in the market space for traditional hosting solutions.

None of the hosting providers is in a position to offer protection against distributed Denial-of-Service (dDoS) attacks. Minimal efforts have been undertaken to throttle ICMP “ping” traffic, however, an analysis shows that the dDoS attacks are application-based on the HTTP TCP port

Melior, Inc.

United States of America – Europe – Asia
US HQ: 1501 Beaumont Street, Dallas, Texas 75215
www.MeliorInc.com – www.dDoS.com – www.BGP4.com – www.Secure.SH
Tel +01-214-421-5975 Fax +01-214-421-5951

80, interfering with regular HTTP requests. The same approach is true for DNS attacks on UDP port 53.

The only logical conclusion is to host the website "english.aljazeera.net" (and others under attack) in an environment which is safe against Denial-of-Service attacks.

2. About Melior, Inc. – Background

Melior, Inc. is a highly specialized computer security company with a long history of providing high-end security solutions, with its roots dating back to 1987 to Germany. In 1996, Melior moved to the United States, and has recently – with the development of iSecure – transformed from a services company to a product company with augmenting services.

Melior is headquartered in Dallas, Texas, USA, with offices and technical personnel in Europe and India.

Melior personnel has a rich background in infrastructure and security; it has built a \$20m data center in San Jose (Silicon Valley, 1998/1999), designed and implemented the worldwide infrastructure for the Macromedia Shockwave Downloads (1995/1996), linked merging banks together (Bank of America & Nations Bank, 1998), deployed the first Point-of-Presence co-lo replication servers on the Internet (1996), and made recently Internet history again by launching the first dDoS-safe hosting environment and demonstration web server (2003).

Melior is currently the only company on the Internet to offer a fully cloaked hosting solution, which is safe against all forms of Denial-of-Service attacks (bandwidth flooding, network attacks, and application-level attacks).

3. About Melior's iSecure CyberWarfare Defense Product

iSecure was developed to protect against Denial-of-Service attacks, one of the oldest and easiest forms of Internet attacks, and also the most devastating. In its distributed form, a dDoS attack is launched from a source behind many "handler" or agent systems, and can only be stopped by the attacker.

All other solutions in the market have taken the approach to combine existing technologies in an attempt to defend against dDoS attacks, by using Intrusion Detection Systems (IDS), Quality-of-Service systems (QoS) to detect attacks and throttle traffic. These systems fall short by design, as they are:

- Signature based (recognize only known forms of attacks, and of those only attacks for which signature files can be written; new attacks are not recognized)
- Slow (the very best response time is 4 minutes, typically 15-45 minutes – the damage is already done within a few minutes or less)
- Often require human interaction, further slowing response time down
- Even in the event of successful detection and reaction, network traffic is throttled, which means the dDoS traffic is overwhelming the desirable traffic: in essence, the dDoS attack is still successful
- Effective only against flooding attacks, no solution for network - or application attacks

Melior, Inc.

United States of America – Europe – Asia
US HQ: 1501 Beaumont Street, Dallas, Texas 75215
www.MeliorInc.com – www.dDoS.com – www.BGP4.com – www.Secure.SH
Tel +01-214-421-5975 Fax +01-214-421-5951

3a. Product Description

iSecure is a stand-alone system, deployed either upstream in the carrier-grade version, or locally in front of the firewall (no security policy violation). It functions as an in-line scanner, inspects the bit-stream traffic and reacts in real time (defined as 6 nanoseconds to 6 milliseconds). It does not use a signature base, but has an intelligent decision engine, which is able to detect “good” and “bad” traffic. Without the need of a signature base, it defends successfully against known and unknown attacks.

iSecure is currently available in three versions for real-time throughput at true 100 Mbit/s, 400 Mbit/s, and 1 Gigabit/s (1,000 Mbit/s).

It has been fully developed, tested in various environment, has never produced “false positives”, works right out of the box, and (optionally) allows for additional configuration, and an administrative interface.

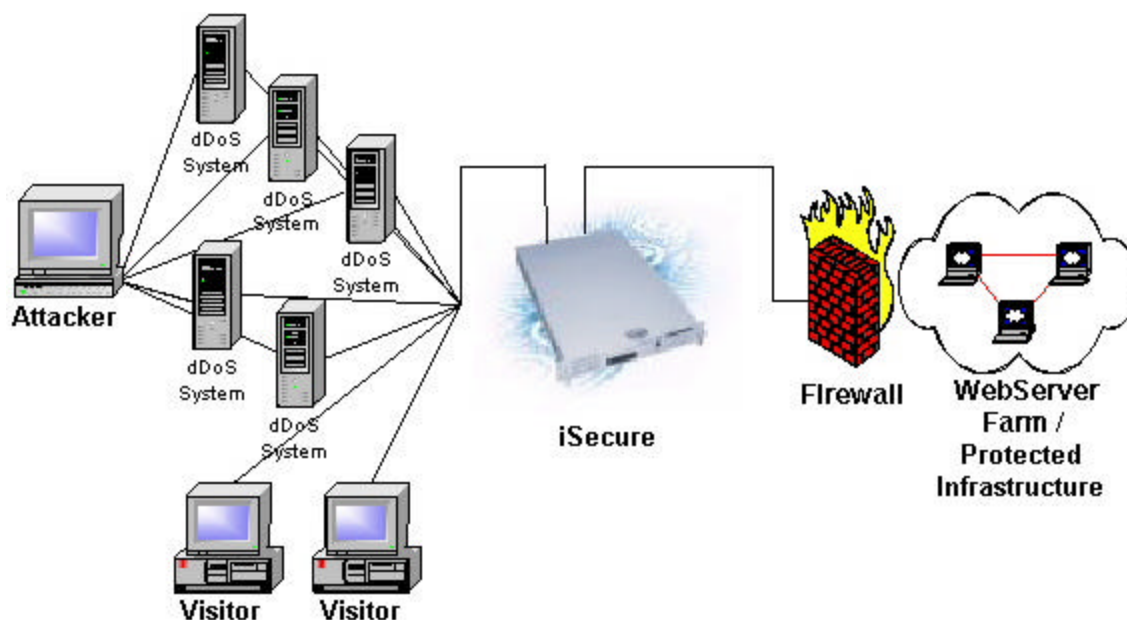


Figure 1 – Deployment Overview

Melior, Inc.

United States of America – Europe – Asia
US HQ: 1501 Beaumont Street, Dallas, Texas 75215
www.MeliorInc.com – www.dDoS.com – www.BGP4.com – www.Secure.SH
Tel +01-214-421-5975 Fax +01-214-421-5951

3b. Functionality: distributed Denial-of-Service Defense

“Bad” traffic is defined as (distributed) Denial-of-Service attack, malformed packets, reconnaissance traffic, spoofed IP numbers, and so forth. Upon detection, it drops the “bad” traffic, while letting the “good” (valid) traffic through.

Detection and Routing of packets is performed in real time (6 nanoseconds to 6 milliseconds at full bandwidth utilization). Valid packets are allowed through to the firewall and the protected infrastructure, while invalid packets and Denial-of-Service attack traffic is discarded.

The protected infrastructure works at normal performance and is not affected by the attack. Visitors from the Internet to the site have access to the content without impact, while the Denial-of-Service attack has no effect:

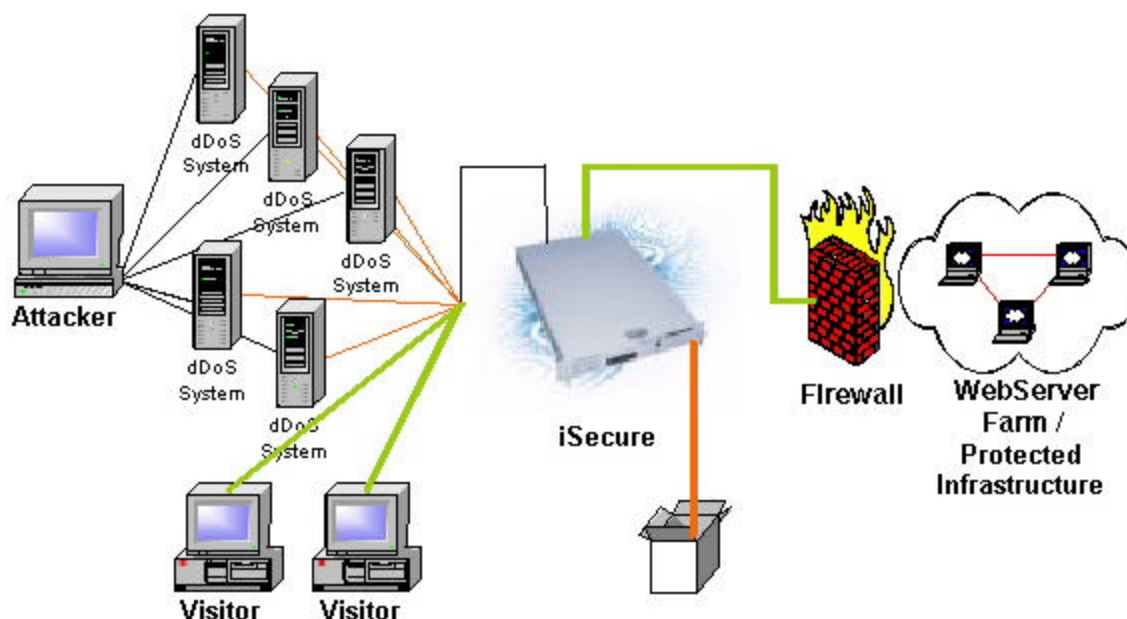


Figure 2 – distributed Denial-of-Service Defense

iSecure defends against all three types of distributed Denial-of-Service (dDoS) attacks:

- Bandwidth Flooding (such as ICMP floods)
- Network Attacks (such as “ping echo” attacks)
- Application Attacks (mixing with port 80 or port 53 traffic)

By covering all three forms of attacks, any dDoS attack from simply script attacks to sophisticated, targeted attacks by any level of expertise of the attacker, as well as with a large number of dDoS “handler” systems, remains unsuccessful.

Melior, Inc.

United States of America – Europe – Asia
US HQ: 1501 Beaumont Street, Dallas, Texas 75215
www.MeliorInc.com – www.dDoS.com – www.BGP4.com – www.Secure.SH
Tel +01-214-421-5975 Fax +01-214-421-5951

3c. Functionality: Infrastructure Cloaking

iSecure also offers another unique functionality: infrastructure cloaking. As the first step of every hacker is first to launch information gathering probes to determine which firewalls, servers, and configurations are in use, making this information unavailable is the first line of defense against attacks of any kind.

All existing solutions in the market are unable to provide this layer of protection. Every firewall limits the number of available ports, however must keep those ports open, which are necessary for communication with the public (visitors). These open ports offer the ability for a hacker to launch exploit and reconnaissance tools. The firewall itself also remains open for mapping and exploitation.

iSecure recognizes any attempt to gain information of the infrastructure it protects, and responds with all ports as “open”, and does not reveal any configuration information. While the production infrastructure performs without impact, no information is revealed to probing attempts, and the attacker has to guess which systems are actually deployed – leaving only guesswork as to which vulnerabilities may exist for exploitation.

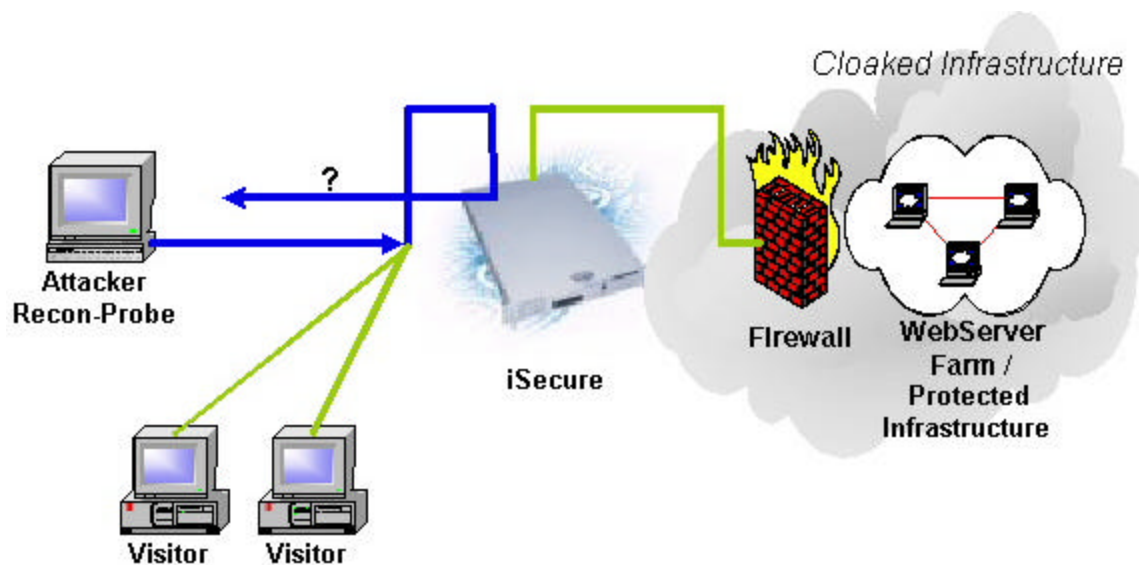


Figure 3 – Infrastructure Cloaking Overview

This unparalleled cloaking feature is the basis of disabling attackers from launching targeted attacks. All Melior hosting services are protected by it.

Melior, Inc.

United States of America – Europe – Asia
US HQ: 1501 Beaumont Street, Dallas, Texas 75215
www.MeliorInc.com – www.dDoS.com – www.BGP4.com – www.Secure.SH
Tel +01-214-421-5975 Fax +01-214-421-5951

3d. Demonstration & Proof

Melior provides many means to prove our security claims for distributed Denial-of-Service Protection and Infrastructure Cloaking:

- ✓ Providing Melior's technical White Paper
- ✓ Demonstration Video for live access on the Internet (streaming media)
- ✓ Demonstration Video on DVD (all region codes) in high-resolution, by request
- ✓ Live Online Demonstrations on our demo system on the Internet
 - demonstration by Melior Technical Staff
 - live test by external parties
- ✓ Live Demonstration at the Melior Data Center in Dallas
 - on Melior-provided attack- and target systems
 - customers and bring their own test tools, attack- and target machines
- ✓ Live Demonstration at a customer site
- ✓ Providing documentation from extensive tests performed at large financial and commercial institutions in the United States and Europe

Melior, Inc. was also just accepted as a member to the SPOCK program, which is a forum consisting of the US Department of Defense, various US Government Agencies, and US Government contractors.

All this information and links to the demonstration video are available on our web site. This weekend, we are in the process to move the last of our California data centers to the Dallas data center, to provide this production environment also with iSecure protection.

4. About Melior's Hosting Solutions

Since 1996 Melior provides highly secure, and highly available websites to customers in Europe, the United States, and Asia, for customers spanning a wide field of industries.

With iSecure, our Hosting environment is safe against distributed Denial-of-Service attacks, and fully cloaked.

We provide solutions for high volume customers, and customize the environment to meet our client's demands. Each hosting environment is carefully designed to perform best for each customer. This includes single or distributed sites, consideration for content delivery to different regions on the globe, appropriate peering agreements, path redundancy, and other vital components.

Melior provides log analysis and trending for up to one year of traffic, which is daily updated, and available via web browser.

4a. Reliability

Melior provides high uptime, for both the infrastructure in itself, as well as traffic management to and from the internet. Redundant servers for web hosting, DNS, E-Mail, etc ensure that even hardware failures do not impact system performance.

Melior, Inc.

United States of America – Europe – Asia
US HQ: 1501 Beaumont Street, Dallas, Texas 75215
www.MeliorInc.com – www.dDoS.com – www.BGP4.com – www.Secure.SH
Tel +01-214-421-5975 Fax +01-214-421-5951

All systems run on highly reliable UNIX platforms, which support all applicable server extensions, including all Microsoft-specific extensions.

Our qualified staff is ready to assist with configuration and setup of customized web content.

4b. Availability

We offer highly available systems either in a single data center, or load balanced across multiple data centers. We own the domain BGP4.com, which stands for the routing protocol which runs the entire Internet backbone (Border Gateway Protocol v4), and offers a redundant infrastructure with distributed Domain Name Servers (DNS), redundant routing access, and dynamically updated configurations.

Our 7x24 support staff guarantees that any arising issues are promptly addressed, and our customers get the best support, true to our company motto: "Perfectionists At Work."

All Melior hosting solutions are protected by our iSecure product, and thus safe against Denial-of-Service attacks, ensuring no service interruption occurs due to outside interference.

4c. Security

With Melior's extensive and proven security consulting experience since 1987, all our own systems for hosting solutions are completely secured and locked down. We deploy the most effective firewall, web server, and e-mail systems, use extensive encryption and LDAP authentication systems, and ensure that our customers get the full benefit from our experience.

Melior has experience in hosting media sites, e-commerce and health care sites, and other industries which rely on secured systems to protect customer and vendor data, as well as avoid changes or defacements of content.

4d. Secure Management by Customer

Our customers have the ability to manage their own configuration for DNS hosts, e-mail accounts, and web content configuration. Melior staff is also readily available to perform any configuration as requested.

Customer access for management and content uploads/changes is SSL encrypted and authenticated via LDAP, to make sure only approved changes occur. Melior also monitors access closely, as a fail-safe check for unauthorized access attempts.

All access and changes are recorded, and logs are maintained for an extensive period. If any unauthorized access attempt is observed, Melior records all forensics information and initiates or assists in legal action as requested by the client.

Melior, Inc.

United States of America – Europe – Asia
US HQ: 1501 Beaumont Street, Dallas, Texas 75215
www.MeliorInc.com – www.dDoS.com – www.BGP4.com – www.Secure.SH
Tel +01-214-421-5975 Fax +01-214-421-5951

5. Proposed Solution: Immediately (Hosting in current Melior facility)

Since the web site "english.aljazeera.net" is currently mostly unavailable (only the cached home page appears, most subsequent links are unavailable), immediate action to restore content is needed.

To make Al Jazeera content immediately available, Melior can host the web site out of its Dallas Data Center within two days, which includes the DNS updates.

With this location and provider change, the Al Jazeera website is protected against Denial-of-Service attacks, and resides on a high-availability platform to handle the traffic of a high-profile web presence. Melior will ensure that upstream bandwidth flooding is protected as well by our co-location provider.

We will need some data on your current bandwidth use to determine the cost. Please provide us with an overview of your bandwidth utilization, web hits, and page views. Based on the information, we may have to upgrade server platforms and infrastructure to handle all traffic, and will provide you within hours with a quote, as soon as we receive your bandwidth utilization data.

6. Proposed Solution: Short-Term (Hosting in carrier-neutral facility)

After the immediate fix, location at a carrier-neutral facility is the next logical step to expand the redundancy by carrying the web traffic across multiple different backbones. This enables Melior to better protect the upstream links and balance the traffic across multiple carriers.

By that time, we have a much better understanding of the traffic patterns, sources of traffic, and can better determine with you if more than one data center location is needed, to cover geographical distribution.

If more than one location is necessary, we can set locations up around the globe, and balance the traffic between them, for optimal performance.

The cost for this solution will be determined by the desired configuration.

7. Proposed Solution: Long-Term (Hosting in Qatar)

You expressed interest in an option to host the AL Jazeera websites out of Qatar. If you determine this is the best solution for you, we can advise and assist you in building out the data center facility, establish the peering agreements necessary for availability, and provide you with the iSecure product, to ensure protection against Denial-of-Service attacks, and full infrastructure cloaking.

With the demonstrated experience at Melior, we have the skill set and the staff around the world to help you effectively with your long-term plans for your web presence.

Melior, Inc.

United States of America – Europe – Asia
US HQ: 1501 Beaumont Street, Dallas, Texas 75215
www.MeliorInc.com – www.dDoS.com – www.BGP4.com – www.Secure.SH
Tel +01-214-421-5975 Fax +01-214-421-5951

8. Other Issues

With the media exposure and failure of several previous hosting providers to keep your web sites available on the Internet, a few other issues need to be discussed.

8a. Why does Melior offer hosting services to Al Jazeera?

At Melior, we are very aware of the extra technical management efforts this particular hosting project introduces. A higher-than-normal hacker activity is to be expected, and more staff has to be dedicated for monitoring, forensics gathering, and customer support.

We do we come forward and offer the service to Al Jazeera anyway? Melior introduces break-through technology with iSecure, for both distributed Denial-of-Service protection as well as Infrastructure Cloaking. Several other companies have offered products over the last year, which are all based on old, existing technologies, and do not deliver the desired functionality. If we can prove that we can successfully protect Al Jazeera, we provide an excellent showcase for every other potential customer interested in this new iSecure technology. In return, we ask to be permitted to add AlJazeera to our customer testimonials web page, a joint press release, and the continued opportunity to earn your business.

8b. No US Export Restrictions

Though Melior, Inc. is a US-based company and part of the SPOCK program, our patents originate in Europe, and we can manufacture and ship products from Europe. Export of iSecure products does not violate any US export restrictions, but shipments from the US to the Middle East may take a longer time for the next months; this delay will not be introduced for shipments from Europe. We do not believe this to be an issue at all, but want to mention it here for due diligence.

Our patents are granted/pending in the European Union, Switzerland, the United States, and all World Trade Organization (WTO) countries. Qatar joined the WTO in 1996, so this does not introduce a limitation.

Product export will only be a matter of consideration for the proposed long-term solution, and thus not any issue for the immediate future.

8c. Political Considerations

Due to the conflict in the Middle East, some political controversies may arise. Al Jazeera has been recognized as an independently and fairly reporting media source, and is funded by the State of Qatar, which is considered a "friendly" nation. Melior provides sophisticated, high-tech solutions, and does not have any objections for content, as long as it is not illegal.

Therefore, we do not believe political considerations are an issue, and we will present it as such, in the event media coverage reflects on it.

Melior, Inc.

United States of America – Europe – Asia
US HQ: 1501 Beaumont Street, Dallas, Texas 75215
www.MeliorInc.com – www.dDoS.com – www.BGP4.com – www.Secure.SH
Tel +01-214-421-5975 Fax +01-214-421-5951

8d. 7x24 Support Available via US (Dallas) or India (New Dehli)

Due to the time difference, we provide support out of our US location in Dallas as well as from India. Our support goes beyond technical considerations, we are also available to handle media events, business issues, and related support, should this become necessary.

Melior can quickly scale up operations in India to meet increasing demands for customer support.

9. Next Steps

Please comment on our proposal, so we can customize our offer to meet your plans.

We will need some information on your current bandwidth use in order to prepare a detailed quote for the hosting expenses.

Additional information regarding the hacking attacks you have observed so far are also desirable to prepare our staff as best and detailed as possible.

For Melior, Inc.

Thomas J. Ackermann, Founder and CEO

Matt Gair, Co-Founder and Vice President Strategic Business Development

John Danchak, Enterprise Sales

Melior, Inc.

United States of America – Europe – Asia

US HQ: 1501 Beaumont Street, Dallas, Texas 75215

www.MeliorInc.com – www.dDoS.com – www.BGP4.com – www.Secure.SH

Tel +01-214-421-5975 Fax +01-214-421-5951