April 2016

A Review and Analysis of the World of Cyber Terrorism

The review discusses the definitions of cyber terrorism, main actors, technological trends, possible risks and recommended ways of coping.

Written by Ami Rojkes Dombe and Yoram Golandsky

Picture source: The Guardian
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Cyber terrorism</td>
<td>4</td>
</tr>
<tr>
<td>Political objectives</td>
<td>4</td>
</tr>
<tr>
<td>Communication</td>
<td>4</td>
</tr>
<tr>
<td>Propaganda</td>
<td>5</td>
</tr>
<tr>
<td>Finances</td>
<td>5</td>
</tr>
<tr>
<td>Fundraising</td>
<td>6</td>
</tr>
<tr>
<td>Recruitment</td>
<td>6</td>
</tr>
<tr>
<td>Acquiring knowledge</td>
<td>6</td>
</tr>
<tr>
<td>Arms procurement</td>
<td>7</td>
</tr>
<tr>
<td>Intelligence gathering</td>
<td>7</td>
</tr>
<tr>
<td>Actors in the world of cyber terrorism</td>
<td>7</td>
</tr>
<tr>
<td>Russia</td>
<td>7</td>
</tr>
<tr>
<td>China</td>
<td>8</td>
</tr>
<tr>
<td>Iran</td>
<td>8</td>
</tr>
<tr>
<td>North Korea</td>
<td>9</td>
</tr>
<tr>
<td>Syria</td>
<td>9</td>
</tr>
<tr>
<td>Hezbollah</td>
<td>9</td>
</tr>
<tr>
<td>Islamic jihad</td>
<td>10</td>
</tr>
<tr>
<td>ISIS aka Daesh</td>
<td>10</td>
</tr>
<tr>
<td>Anonymous</td>
<td>10</td>
</tr>
<tr>
<td>Technological Trends in cyber terrorism</td>
<td>11</td>
</tr>
<tr>
<td>Encryption</td>
<td>11</td>
</tr>
<tr>
<td>Biometrics</td>
<td>12</td>
</tr>
<tr>
<td>Malicious Software</td>
<td>12</td>
</tr>
<tr>
<td>Command and Control</td>
<td>12</td>
</tr>
<tr>
<td>Big Data &amp; Algotrading</td>
<td>13</td>
</tr>
<tr>
<td>The main risks of cyber terrorism</td>
<td>13</td>
</tr>
<tr>
<td>Critical infrastructures</td>
<td>13</td>
</tr>
<tr>
<td>The Financial Sector</td>
<td>14</td>
</tr>
<tr>
<td>Communications</td>
<td>14</td>
</tr>
<tr>
<td>EMP</td>
<td>14</td>
</tr>
<tr>
<td>Countering Cyber terrorism</td>
<td>14</td>
</tr>
<tr>
<td>Conclusion</td>
<td>15</td>
</tr>
</tbody>
</table>
Introduction

In order to conduct a discussion about cyber terrorism, one needs to differentiate between terrorism and other kinds of threats in cyberspace, such as organized crime, espionage, cyber war and activism. Terrorism is characterized as an act intended to achieve political objectives through influencing the decision making process of a nation state. Another characteristic is that it is an act intended to cause fear through violent means. For instance, activism also wants to affect political decision, but does not use intimidation of the public to do so.

Violent means that are used in cyber terrorism can physically harm people through manipulation of information systems (IT&OT) that run physical systems [critical infrastructures]. They can also be used to disrupt the routine of modern life that is based mostly on information systems [for example, attacks on the financial sector].

Another point to be taken into consideration when reading this review is that a cyber terrorist organization operates in a very similar way to a business organization. In both cases, it is a for-profit organization, but instead of financial gain, the terrorist organization is acting to achieve political gain. This means that many of the tools and methods used by business organizations in the cyber sphere for financial gain are used by the terrorist organization to gain political objectives. This dual use of technologies, tools and methods makes it difficult to identify and counter cyber terrorism.

Terrorism is an act of very high intensity in terms of the risks it entails and possible impact, in addition to undermining the public's sense of security. It is usually performed in the context of an organization, one that may be strong, secretive and many times benefits from global network and the lack of physical boundaries, as well as the support of the local population.

Most definitions of a terrorist act are based on a number of premises:

- The purpose of the act is to promote a political, ideological or religious purpose.
- The goal of the act is to create an effect of extreme fear and panic in the general public or force a government/elected body to change its policy.
- The act is characterized as a grave and violent one that can endanger human life (also through the disruption of critical infrastructures).

Professor Boaz Ganor of the International Policy Institute for Counter-Terrorism defines terrorism as "a violent struggle, in which violence is used intentionally (or threatened to be used) against civilians, for the purpose of achieving political goals".

---

Cyber terrorism

Cyber terrorism is no different in its objectives than physical terrorism. Cyber terrorism uses the cyber sphere to spread fear and panic in the general public in order to achieve political goals. Unlike physical terrorism, cyber terrorism has yet to directly cause fatalities.

Terrorism uses cyberspace for more pragmatic purposes as well, such as fundraising, recruitment, acquiring knowledge, intelligence gathering, money transfer, arms procurement and purchasing of other goods. In fact, a terrorist organization uses the cyber sphere for every aspect necessary to run its operations, just like any legitimate business.

Cyber terrorism is less expensive to execute than physical terrorism. One reason being awareness. While terrorism in the physical sense is not a new phenomenon and nations have established intelligence and defense organizations to deal with it and foil it, terrorism in the cyber sphere is a relatively new phenomenon that has yet to create national or international mechanisms to counter it. Therefore, in economic terms, the threshold for committing cyber terrorism is lower than in physical terrorism.

Cyber terrorism does not require a long, complex and expensive logistical tail. In theory, any lone wolf/hacker with a reasonable resources can commit an act of cyber terrorism while drinking espresso in a coffee shop. Hacking the twitter account of the president of the United States and posting a threatening message does not require prolonged intelligence gathering, explosives, weapons, a getaway car or safe houses.

Political objectives
Cyber terrorism is mostly employed by the same actors who perform terrorist acts in the physical world – terrorist organizations and nations who sponsor terrorism. Its main objective is to achieve political gain.

The main tool in cyber terrorism is spreading fear in the public. The main methods of doing so includes media websites, social networks and websites/blogs belonging to leaders of public opinion. The terrorists will seek out the platform with the greatest ability to spread a threatening message to the public. It is not a coincidence that "The electronic Syrian army" a terror group associated with the Assad regime in Syria, is known for attacking twitter accounts of news channels.

Communication
One main use of the cyberspace in terms of terrorism is for communication purposes – for contact between operatives to execute an attack in the physical dimension, recruitment, planning a collective cyber-attacks, or passing messages for any other purpose.

---

The technologies used to this end are those utilizing electromagnetic transmissions and those using the internet - from landline, mobile and satellite phones, VOIP communications based on SIP protocol or any other medium. The internet communication tools are chat programs [WhatsApp, Viber, Telegram and others].

One should remember that when it comes to communication there is no real difference between the operations of a terrorist organization and a business organization, the difference is in the objectives. While the former wants to spread fear in the public, the latter wants to sell a product to the public. In both cases this means selling an idea for the purpose of motivating the end consumer to act. Therefore, when thinking about the use terrorist organizations make of cyber, one should assume they will use similar tools to those of a business organization. Thus we learn about one of the most basic problems of dealing with and foiling cyber terrorism - the dual use of technology. In other words: the same technology that is used for legitimate economic activities, can be used for terrorist activities.

Propaganda

Terrorists want to spread fear. Hence they direct their activities at news outlets that can mass distribute messages to the public with little effort. To this end terrorist organizations use websites of media outlets, companies and individuals who are thought leaders on social media. Another platform to pass on a message to the masses is by cell phone. There were cases in the past in which Hamas has sent threatening text messages to the Israeli public.

Propaganda can be achieved through creating messages in the physical dimension. For example, if a terrorist organization can gain control over the traffic light system and obstruct the main roads, it will convey a powerful message. It can also do so by disrupting information on a commonly used navigational system like Waze. Proving the capability to disrupt the daily routine can cause fear in the public and gain political capital.

In the age of internet of things [IOT], terrorist organizations can use any technology that delivers messages and is connected to the World Wide Web - for example, electronic billboards, smart TVs and others. In terms of propaganda, the advantage a terrorist organization has in cyberspace is the relative ease of disrupting messages conveyed to the public. For example, hacking the twitter account of a prime minister is not considered a very difficult task, but its results can be devastating.

Finances

The financial sector is used by terrorist organizations for two main purposes: financial management of the organization and attacking of the financial sector to disrupt normal life and cause fear. In the management aspect, the terror organization uses the banking system for money laundering, payments to operatives, arms procurement, payment for cyber-attacks conducted through outsourcing and various other missions.

3 “ISIS Engineers and Scientists Collaborate on Projects in ...” 2016. 27 Mar. 2016
When it comes to causing fear, the terrorist organization will act to disrupt life’s routine: disrupting the stock exchange, altering data bases of a central bank or manufacturing a bribery case for an elected official through the injection of information into his bank account - all of these can cause chaos in a country. The financial sector can be a mean of spreading fear in the public due to its pivotal role in everyday life.

Another technology used in the financial sector is virtual currency which by design is a method of transferring funds anonymously. Terrorist organizations use this medium to make it more difficult for national an international security services to track their sources of funding.

Fundraising

As any other organization, terrorist organization needs funding to execute its ideology, funding typically come from a supporting nation (when associated) and from "donations of ideologist supporters, the same way the WWW is perfect for fundraising in Kickstarter it is perfect for fundraising terror operation. Instead of sending representatives door to door a terror group sends an email or a message through social media groups. The purpose is the same – reaching out to a supportive audience and raising funds. Digital currencies such as Bitcoins help the organization raise funds anonymously.

Fundraising among supportive communities might be legitimate act (pending on the purpose). However, knowing that it exists should lead to monitoring these activities in order to uncover the ways that terrorism is funded. Furthermore, contacts that are made for the purpose of fundraising can also be used for other purposes, such as recruitment, intelligence gathering, arms procurement and more.

Recruitment

Recruiting operatives is similar in its essence to fundraising, only instead of funds the resource is operatives for the organization. For example, ISIS recruits operatives through twitter[^1] or Anonymous recruiting operatives to attack Israel on April 7th with a DDoS attack. Recruitment is done on online forums, mailing lists, and any other means that enable the terrorist organization to contact its loyal public.

Acquiring knowledge

Terrorists need to learn - whether it is knowledge for physical implementation of terrorism [building bombs, working with explosives] or knowledge for implementation in cyber terrorism [programming languages, coding malicious software]. The cyber sphere that is used as an infrastructure for knowledge sharing is also used by those engaged in terrorism to acquire information and knowledge.

Alongside tactical information, the internet allows terrorists to acquire academic knowledge in the fields of engineering, chemistry, physics, etc. Higher education enables terrorist organization to close technological gaps they have compared to the capabilities of a nation state. In the

context of cyber, higher education in the fields of sciences and computer sciences places the terrorists in the forefront of knowledge, alongside white hat hackers.

Arms procurement

The cyber sphere is used by terrorists to procure physical weapons and cyber malicious software. Whether through secret groups on social media, closed forums, IRC channels or the dark web, arms procurement is an industry serving anyone with money.

For a number of years criminal organizations have dealt in the commercialization of malicious software. This is an huge industry engaged in the development of malicious software sold as a service [SaaS], including support and updates. Modern malicious software is composed of a collection of components put together to create an attack tool as a service. Each such component is an entire professional field, with developers who do it for a living. This is a full economic ecosystem of professional service providers collaborating amongst themselves for the purpose of selling malicious software. This commercial infrastructure is used by cyber terrorists. Alongside purchasing of cyber-attack capabilities, there is also an infrastructure based in the cyber sphere for buying and selling physical weapons of various kinds.

Intelligence gathering

The WWW is awesome for intelligence gathering, the terrorists acquire intelligence on their targets from 3rd parties, collect OSINT and WebINT, map-out targets, plan courses of action in preparation for an operation and use the internet to coordinate operations. In fact, there is no difference between a business organization wanting threat intelligence for defensive purposes, and a terrorist organization wanting intelligence for the purpose of preforming a "cyber terrorist attack". In both cases intelligence gathering can be performed through the same tools and methods.

Actors in the world of cyber terrorism

Russia

Russia is considered one of the countries that possess superior cyber capabilities. Russia first used cyber as a weapon during the war with Georgia in 2008. Subsequently Russia started using cyber terrorism as a means of promoting its political objectives. One example is the attacks on critical infrastructures in the Ukraine executed by a group typically associated with cybercrime.

8 "Ukraine says to review cyber defenses after airport targeted …" 2016. 26 Mar. 2016 http://www.reuters.com/article/us-ukraine-cybersecurity-malware-idUSKCN0UW0R0
9 http://freebeacon.com/issues/fbi-warns-cyber-threat-electric-grid/
Russia is used as a shelter for companies offering "Bulletproof Hosting"\(^{10}\), many of whom are used as an infrastructure for cyber terrorist attacks alongside gambling and child pornography. Russia is also home to some of the largest cyber-crime organizations in the world. These criminal organizations are also used as part of the infrastructure for executing acts of cyber terrorism.

**China**

China is also considered one of the countries that possess superior cyber capabilities. China is estimated to employ nearly 200,000 people in the field of cyber, about 30,000 of them work for the Chinese army and the rest in the private sector\(^{11}\). Officially, China opposes any kind of cyber terrorism, but unofficially it has the ability to disrupt critical infrastructures, banking systems and the systems for relaying information to the public [news media]. Hence, it has great potential for using cyber terrorism for political purposes, those capabilities might materialize if the United States chooses to threaten the stability of the ruling communist party.

**Iran**

Iran is known to employ terrorism for political purposes. For the most part, Iran's cyber terrorist attacks correspond to political maneuvers it is trying to promote, for example whilst the nuclear talks with the US and Europe. During the negotiation talks Iran employed a variety of cyber terrorist acts against the US\(^{12}\).

Iran has developed very good cyber capabilities over the years, and these are displayed in its ability to apply cyber terrorism. One way to enhance these abilities is to disrupt or threaten critical infrastructures.

Cyber terrorist attacks that can physically damage critical infrastructures of a country can cause grave casualties and lead to panic in the public. One such example is the Iranian attempt to target a dam in the state of New York\(^{13}\).

Iran is considered one of the strongest countries in terms of cyber capabilities. This is due to a sound academic infrastructure, a well-developed military industry and high motivation to use terrorism as a political tool\(^{14}\). Iran also uses terrorist organizations as a proxy [Hezbollah for example] and therefore it can implement cyber terrorism through them as "proxies" without the trail leading back to Tehran. Also in Iran there is an apparent connection between the government and private hacking groups that are used in order to execute the Iranian cyber strategy.

---

10 https://en.wikipedia.org/wiki/Bulletproof_hosting


North Korea

North Korea employs terrorism for political purposes. The one event that placed the country on the terrorist map and in the news was the hacking of the Sony Corporation\textsuperscript{15}. An attack that came as a response to a movie that Sony produced that mocked the ruler of North Korea. North Korea also uses cyber terrorism to cause fear in South Korea. Among other incidents, it tried to attack train infrastructures\textsuperscript{16} and nuclear power plants\textsuperscript{17}. More about the capabilities of North Korea can be found in a report by the CSIS website\textsuperscript{18}.

Syria

The Assad regime uses cyber terrorism through a hacker group called "the Electronic Syrian Army". It is estimated that this organization receives funding from the Syrian government. One incident attributed to this organization is an attempt to poison the water system in Israel. The Electronic Syrian Army is known for its specialty in attacking news organizations\textsuperscript{19}. Their purpose is to broadcast messages through news outlets to promote the political goals of the Assad regime. This organization also engages in exposing the classified information of various regimes in the Middle East\textsuperscript{20}. There is no doubt this organization is aware of the strength of the media as a medium for employing terrorism and specializes in it.

Hezbollah

Hezbollah is a terrorist organization, employed as an Iranian extension, and therefore it is assumed that technical capabilities from Iran are transferred from Iran to Hezbollah. This transfer includes training of human capital in cyber, procurement of tools and systems, and sharing of intelligence knowledge. Hezbollah's cyber capabilities were exposed in 2006 when during the second Lebanon war with Israel a claim was made that the organization was able to hack into the IDF's encrypted mobile network called "Vered Harim".

In 2013 there were claims that Israel eliminated the head of technology of the organization. This exemplifies how in the cyber sphere, technological capabilities that reach the hands of a terrorist organization, can pose a threat to an official state.

In February 2016 the organization unveiled its hacker unit and its capabilities, claiming to have superior capabilities.

\textsuperscript{15} "How the U.S. Knew North Korea Was Behind the Sony Hack ..." 2015. 26 Mar. 2016
\textsuperscript{16} "North Korea denies cyber-attacks on South Korea officials ..." 2016. 26 Mar. 2016
\textsuperscript{17} "North Korea Blamed for Nuclear-Power Plant Hack - WSJ." 2015. 26 Mar. 2016
\textsuperscript{18} "Executive Summary: North Korea's Cyber Operations ..." 2015. 26 Mar. 2016
Islamic jihad

The Islamic jihad is a terrorist organization operating in Gaza and has adapted cyber capabilities. Mostly it is an infrastructure based on "talents" – few individuals with high technical capabilities. This is not an organized infrastructure that develops human capital to perform cyber activities. Not much is known about the organization’s cyber capabilities, but a case that was revealed in March 2016 shed light on the organization’s capabilities. In that case, a hacker named Majed Awida was accused of developing hacking software to infiltrate monitoring systems and sensitive systems of the military, police and TLV Airport. According to the charges, Awida, a computer engineer by profession, developed hacking software through which one can watch the live video of traffic cameras and police camera, and thus locate crowded places, assembly places of security forces and follow traffic cameras in Israel. The indictment also attributes to Awida the development of software enabling the tracking of aircraft and passenger movements in TLV airport. According to the indictment, Awida supplied the software to the Islamic Jihad and has continued developing malicious software for the organization that would enable the organization's high ranking officers to track the IDF’s UAV transmission in real time.

ISIS aka Daesh

Operating in Syria and Iraq, uses the cyber sphere mostly for the purpose of intimidating the world’s population and creating propaganda. The most prominent example is the posting of horrifying executions in various methods on social media. The organization's use of cyberspace for the purpose of publicizing its extreme visual messages is considered "pure" cyber terrorism, aimed at causing fear. Alongside posting threatening messages and propaganda, the organization uses cyberspace for the routine operational activities of recruiting resources and people. In the context of terrorism the organization also uses other methods such as advertising the names of American security personnel with a call to its operatives around the world to assassinate them.

There is no doubt ISIS is aware of the power of cyberspace for spreading propaganda and fear and it works to this end in social media and the internet. The organization also publishes a monthly online magazine named Dabiq uses chat services for communication with operatives and even developed mobile software for encrypted communication.

Anonymous

Anonymous is a terrorist organization operating for political purposes in the cyber sphere. Unlike other terrorist organizations in the physical world that also use cyber capabilities, Anonymous operates exclusively in cyberspace. Anonymous operates on the border between activism and terrorism.


Well known terrorist attacks by Anonymous are the attacks on Israel on April 7th over the past four years. These attacks were intended to spread fear in the Israeli public and effect the political decisions of the Israeli government. Anonymous operates in a similar manner towards other countries through Denial-of-service attack on government or stealing classified information and publishing it in order to intimidate and undermine the regime. Anonymous recently threatened to disrupt the Olympic game of Rio.

**Technological Trends in cyber terrorism**

Similar to the physical dimension, terrorist organizations in cyber space outsource assignments to criminal organizations for payment. It's been established that there is a link between terrorist organizations and organized crime, a link that is based on financial gain. One can also observe a connection between rogue states and terrorist organizations. Another link that was observed is between terrorist organizations and hacking groups that are used as mercenaries.

When examining the technological trends in the cyber terrorism world, it is important to note these links exist and technological trends flow from one group to the other. An emphasis should be made on the flow of technology from the world of organized crime and the world of state cyber capabilities to the world of cyber terrorism. One prominent example is the leak of the Stuxnet code from the world of state-cyber to the internet. This means a code that was created by a nation as a weapon to attack critical infrastructures is now at the hands of terrorist organizations and rogue states supporting these organizations. For those who do not believe a software code can paralyze critical infrastructures, it is recommended they review the experiment the American DHS held in 2007.

**Encryption**

One of the trends we see in the world of cyber terrorism is a growing use of encryption, for the purpose of concealing the terrorists' activities from the state's security services. It is assumed that some of the cyber terrorism organizations have extremely high technological awareness, and therefore know that modern countries develop tools to monitor communications through electromagnetic transmissions and the internet. Voice, data, images, video or text – all are monitored. Therefore, terrorist organizations use encryption to hide their activities. The use of encryption is not limited to a specific medium. From two-way radio devices, laptop and desktop computers, mobile phones, e-mail, chat software or file sharing software, the terrorist organization will try and maintain encrypted communications.

---

23 [http://www.ibtimes.co.uk/brazil-2016-summer-olympics-hacker-group-anonymous-attacks-expected-1549852](http://www.ibtimes.co.uk/brazil-2016-summer-olympics-hacker-group-anonymous-attacks-expected-1549852)


Encryption is not just AES. In the past the Israeli Mossad revealed that terrorist organizations use known websites such as Reddit, eBay and porn sites to pass encrypted messages. In that case the technique is called steganography and it enables hiding information in legitimate files.

Biometrics

Use of biometric technologies is expected to gain momentum in future in the user verification process of technological services. This trend is also expected to come into use amongst cyber terrorist organizations. Much like encryption, biometric technologies can aid terrorists in concealing their activities from law enforcement.

Another aspect of the biometric technology is the ability of terrorist to manipulate data for the purpose of intimidation. The main concern of law enforcement and data security professionals is a leak from a government's biometric database. In theory, this scenario will enable the framing of innocent people. Whether they are thought leaders in the political, business or military world, framing them can undermine the sense of security the general public has in their government. Biometric technologies are also expected to come into use as verification methods in the financial world. For terrorists, possessing such capabilities can give them an advantage in committing financial crimes for the funding of terrorism.

Malicious Software

Terrorists will continue to be part of the cyber ecosystem of malicious software, whether in developing malicious software, buying them or hiring hackers to attack targets on their behalf. It is safe to assume that terrorists will increase their efforts to get their hands on capabilities that can disrupt the operations of critical infrastructures in order to conduct a mass casualty attack or disrupt the day to day life. In the attack in Brussels in March 2016, one of the assumptions is that the terrorists planned to disrupt the operation of a nuclear power plant in Belgium.

In addition to damaging critical infrastructure, malicious software will continue to be used in the terrorist’s tool box for hacking of websites, social media accounts, databases and financial crimes.

Command and Control

Sophisticated terrorist activities in the cyberspace or the physical world require coordination, and the way to achieve it is to use command and control technologies. Cyber terrorists have adopted such technologies for the purpose of coordinating operatives in preparation for an attack, joint intelligence gathering and operational planning.

---


In addition, command and control technologies can aid the terrorist organization in managing equipment stocks, money and knowledge. In the cyber sphere, a terrorist organization can use the Waze Rider service to coordinate a meeting between members of a sleeper cell, despite the fact that the service was originally designed to plan carpool rides to work. And this is just one example.

Big Data & Algotrading
A fascinating and very advance technological field that can be very useful for terrorists is algotrading. Originally, it was intended for developing algorithms for automatic, fast stock trading. However, this field has already come into use in recent years in the military field for improving real-time decision making processes based on information collected by big data systems. Similar to a military organization, a terrorist organization can also use these technologies for real-time decision making, whether they are for cyber terrorism or the physical dimension. The ability to collect large amounts of data to be analysed by the algorithm for decision making is not foreign to terrorist organizations. In the same indictment of an Islamic Jihad operative in March 2016, it was revealed the organization wanted to use the information from Israeli traffic cameras and a mobile app for monitoring airplane traffic in order to increase the damage caused by the rockets the organization launches at Israel.

Using algotrading technology, combined with big data, will provide terrorist with the ability to make better decisions in real time and enhance the impact of damage caused by their activities, and the level of fear they spread in the public.

The main risks of cyber terrorism
To sum up the main risks of terrorism, I will chose to define it as disrupting the routine of life. The political and economic systems operate on the assumption that there is a defined routine which allows stability. If we examine countries that are subject to widespread terrorism, we can observe that they lack stability of those two systems.

From a business point of view, terrorism spreads fear in the consumer public. This fear causes behavioral changes that affect the economic system. That can materialize in effects on the stock market, the consuming habits, long-term financial decisions [such as changes in real estate prices as a result of the frequency of terrorist incidents in a certain location].

From a political point of view, terrorism tries to disrupt the governability of a regime. Political instability also directly affects the economic system both in terms of local consumption, as well as global investments coming into the country.

Critical infrastructures
One of the main risks that cyber terrorism poses is a threat to a country's critical infrastructures [electricity, water, food, medicine]. Damage to these infrastructures can paralyze a country's economic system for an extended period of time.
The Financial Sector

Choosing to define the financial sector of a state as a critical infrastructure is a political choice. It terms of the business owner, one should view the financial sector as a critical infrastructure which, when damaged, can have significant impact on businesses.

Communications

News outlets in various mediums, social media and publications by thought leaders in various fields should be considered a potential target for cyber terrorist attacks. Through publishing of true or false reporting in cyberspace, and propaganda a terrorist organization can inflict extensive damage to a business in the physical world, causing a change in the consumers' behaviour.

EMP

Another threat I have chosen to add to the list is the electromagnetic pulse or EMP. This is a threat that is not discussed much in the media, but it is relevant to the world of terrorism as well as the cyber sphere. EMP destroys all electronic circuits in the attack zone and effectively destroys all computer systems in that area. It's a mean of physical DDoS for computer systems. Recovering from such an attack takes a long time, sometimes months or years. Even though this is a relatively supervised technology, EMP generators in various sizes and shapes can be acquired through organized crime or other terrorist means. This is an extreme scenario, but one that shouldn't be ignored.

Countering Cyber terrorism

Coping with cyber terrorism can be divided into two parts: the first is at the nation state level and the second is the business sector level. Much like the physical dimension, threats at the state level cannot and shouldn't be handled by the business sector. However, the business sector should be aware of the threats, especially those that can affect its business operations. The business sector should assume it is a target for terrorism since it is part of a wider context, for example - businesses in the state of Israel. In this scenario, Anonymous has targeted Israeli business organizations to try and influence political decisions of the Israeli government. Cyber terrorism prevention is almost impossible for a business. However, business should include cyber terrorism as part of its threat modelling and prepare to such attacks.
**Conclusion**

Cyber terrorism is in many ways similar to physical terrorism, this conceptual similarity allows to draw from one dimension to the other. However, there are few main differences. One difference is that it is harder to deter a cyber terrorist organization, one of reasons for this is the problem of assigning responsibility for an attack due to lack of physical (and other) evidence, and when you cannot assign responsibility for a cyber-attack to a specific entity, you cannot punish it, hence no deterrence.

A second difference stems from the fact that cyber terrorism targets the business sector directly. While in the physical dimension the government through its security services has the proper infrastructure to shield the business sector from terrorism, in the cyber sphere the governmental security services are almost none existent and the responsibility for handling cyber terrorism is left with the business owners. This reality forces the organization to be aware of the threats arising from cyber terrorism, and to take the necessary action to defend and recover from it with very little support from the government.

There is no doubt cyber terrorism is a challenge for modern business organizations. The economic connectivity based on the World Wide Web forces business globally to deal with the "butterfly effect" – changes in one place in the world can quickly affect businesses on the other side of the globe, terrorist organizations use this reality to its full.

If credit cards are stolen from a retailer in Europe, and the incident is publicized on the internet, that message goes out to all consumers around the world. This means the sense of security of consumers around to world to shop online is diminished. This behavioral change leads to a drop in proceeds from online transactions thousands of kilometres from the origin of the incident. Cyberspace makes the changes in consumer behaviour into global trends.

The responsibility for dealing with cyber terrorism rests on the shoulders of the business organization. The fact that the government is out of the equation forces the business organization's executive team to prepare and react to such event which is an additional operational and managerial overhead cost that is added to the daily operation of the business not to mention the potential impact that can be caused due to a cyber-attack on public infrastructures of a nation state.

Ignoring the threat from cyber terrorism threat will not make it go away and would certainly not prevent it. Cyber terrorism is here to stay and will almost certainly toll its price from the business sector.