Cyberterrorism: A look into the future
By (ISC)2 US Government Advisory Board Executive Writers Bureau
Infosecurity.com, 12 November 2009
http://www.infosecurity-magazine.com/view/5217/cyberterrorism-a-look-into-the-future/

Cyberterrorism might mean different things to different people, but one thing is certain – it needs to be taken incredibly seriously. What are we dealing with? How can we defend our nation? How will cyberterrorists of the future look to attack? The (ISC)2 US Government Advisory Board Executive Writers Bureau answers these questions

One of the key challenges of understanding 'cyberterrorism' is defining exactly what the term means. The term has been used in the past to refer to known terrorists or terrorist organisations using the internet to communicate.

Currently, the term cyberterrorism more often refers to the act of attempting to damage or exploit cyber networks and their connected computers or the act of attempting to use cyber networks (especially the internet) to wreak havoc and destruction on other targets, which they access through cyber networks. Even the individual terms 'cyber' and 'terrorist' are inconsistently interpreted.

What the experts say
Andrew M. Colarik of the USA and Lech J. Janczewski of New Zealand state that, "In the context of information security, terrorists may come in many forms such as politically motivated, anti-government, anti-world trade, and pro-environmental extremists".1

They further state, "Cyberterrorism means premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programmes, and data that result in violence against non-combatant targets" (ibid).

This interpretation of cyberterrorism creates a distinction between a cyberterrorist and a malicious hacker, prankster, identity thief, cyberbully, or corporate spy based on the political motivation of the attacker. It also differs from hacking, cracking, phishing, spamming, and other forms of computer-related abuse, though cyberterrorists may use these tactics to accomplish their politically motivated goals.

Dr. Dorothy Denning, Professor in the Department of Defense Analysis at the Naval Postgraduate School states that cyberterrorism "refers to the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political and social objectives"2.

According to Dr. Irving Lachow, PhD, Professor of Systems Management at the US National Defense University in Washington, D.C., "While there is clear evidence that terrorists have used the internet to gather intelligence and coordinate efforts to launch physical attacks against various infrastructure targets, there has not been a single documented incidence of cyberterrorism against the US Government."3

It should also be noted that there is another school of thought that says cyberterrorism does not exist and is really a matter of hacking or information warfare. Those who hold this view disagree with labelling it ‘terrorism’ because it is unlikely that these acts cause fear, significant physical harm, or death.

Cyberterrorism definition

Cyberterrorism refers to attacking computers, networks, and other electronic technological capabilities to either damage the cyberspace infrastructure itself or to damage some other target, motivated by terrorism. Cyberterrorism may grow depending on a cyberterrorist’s perceived benefits of using such tactics.

One way it may manifest itself in the future is by applying cyberterrorism tactics to Supervisory Control and Data Acquisition (SCADA) systems, creating the potential (or fear of the potential) for damage to the integrity of the critical infrastructures such as water supply, electrical grid, transportation systems, and financial systems. Such attacks could undermine a population’s faith in its government and in the security of the nation’s critical infrastructures.

To be able to defend against acts of cyberterrorism, we must act now both as a government and as individuals.

How serious is the problem of cyberterrorism?

Ask Estonia. The three-week cyberattack on Estonia threatened to black out the country's digital infrastructure, infiltrating the websites of the nation’s banks and political institutionsiv. What really keeps cybersecurity professionals up at night is not necessarily the threat of shutting down banking and financial infrastructures, rather the concern for the security of Supervisory Control and Data Acquisition (SCADA) systems related to the nation’s critical infrastructures.

These are the industrial controls systems that are managed by computer systems. SCADA systems include railroad track switches, draw bridges, sewage treatment and water purification plants, traffic signals in busy cities, the electrical distribution grid, subway control systems, and other critical systems that can easily cause massive injuries and loss of life if exploited maliciously.

Many of these systems are connected to the internet and run on commonly understood operating systems using well-known, standard communications protocols. In many cases, access to these systems is not controlled as tightly as expected given their potential impact on life and safety.

A concerted, focused cyberterrorism attack on these systems could have a devastating effect on public safety and confidence. If terrorists were to attack a SCADA system simultaneously with physical bombings, public panic could quickly spin out of control. If terrorists were to bomb a busy city intersection while simultaneously shutting down the electrical systems in a nearby hospital – a combined attack known as a ‘force multiplier’ in military terms – this would result in national panic. The impact would be devastating to the surrounding population.

Some recent occurrences of cyberterrorism attacks on these systems include an incident in Romania where a cyberterrorist illegally gained access to the computers controlling the life support systems at an Antarctic research station, endangering the 58 scientists involved. Fortunately, the culprits were stopped before damage occurred.

Most acts of sabotage, while not politically motivated, have caused financial and other damage, as was the case where a disgruntled employee in Maroochy Shire, Australia, caused the release of untreated sewage into water.

If Hollywood and popular fiction resemble future predictions, we might consider how cyberterrorism is being depicted in fictitious scenarios such as in Dan Brown's novel, Digital Fortress, Amy Eastlake's Private Lies, and the Tom Clancy series, Netforce (about an FBI/military team dedicated to combating cyberterrorists).

The films Live Free or Die Hard (a group of cyberterrorists intent on shutting down the entire computer network of the United States) or Eagle Eye (involving a super computer controlling everything electrical and networked to accomplish the goal), and a television episode of 24 which included plans to breach the nation's nuclear plant grid and then to seize control of the entire critical infrastructure protocol, are also examples of how media depicts cyberterrorism.

What can we do about cyberterrorism?
The good news is that there are many highly trained, internationally certified, experienced security professionals thinking about this problem. They are participating in exercises, examining case studies, war-gaming various scenarios, and implementing solutions. These experts from military, industry, and academia work well together and offer a global perspective.

There is also an abundance of policies, practices, tests, hardware, software, literature, training and education designed to protect against cyberattacks, regardless of the source (terrorist or otherwise), to detect it immediately when it happens, and to respond to it quickly and effectively.

The threat of cyberterrorism, however, is similar to the threats of other types of network exploitation, and carries with it warnings. Firstly, while cyber defenders must confront the full range of security vulnerabilities, the cyberterrorists need to succeed in finding and exploiting only a single vulnerability to accomplish their mission. Therefore, the level of effort is significant for the defenders.

Secondly, terrorists are typically passionate about accomplishing their goals, and are often willing to lose their own lives to accomplish massive destruction. However, while many security experts are professionals who take their work very seriously, they are generally not fanatics working 20 hours a day for an extreme ideology.

The third problem is that the internet was not initially designed for confidentiality or integrity (two of the services of security). It was designed for availability and resiliency by providing a packet switched network with alternate paths meshed together. The security services of confidentiality and integrity usually must be implemented at the application and end-point levels (computer, mobile phone, personal digital assistant, etc.).

While we may be somewhat positioned to defend against such acts, we must act now – as a government and as individuals – to fully meet the challenge of cyberterrorism. Some methods we may use include:

1. Implementing strong access control systems to ensure that only authorised individuals can access cyber systems
2. Using strong encryption to ensure confidentiality and integrity of information stored, processed, and transmitted on and through cyberspace
3. Closely monitoring all cyber activity by using log files and log analysers
4. Keeping policies up to date, and ensuring they are strictly enforced
5. Implementing effective detection systems to recognise cyberattacks quickly
6. Appointing active cybersecurity leadership to implement a real-time national defence strategy

The future of cyberterrorism

A critical factor in defending against cyberterrorism is thinking towards the future. It is easy to fall into the trap of projecting what terrorists might do in the future to our current technologies. But, we must think about what terrorists might do in the future to our future technologies. This becomes doubly challenging since predicting the future is always difficult and this challenges us to predict the future in two dimensions. Future terrorists will not attack what we have now.

They will attack what we will have in the future. For example, as we evolve more toward virtual worlds, diskless workstations (‘thin client’), and cloud computing, computing capabilities are being deployed at a national-level utility rather than as individual or corporate data systems. We would be wise to extrapolate into the future based on current trends, then to think about how cyberterrorists might attack our future environment and technology infrastructure.

In his best-selling book, The Big Switch, Nicholas Carr compares current computer trends to those of electricity development. More than 100 years ago, individual factories built their own electrical generators using water wheels by the sides of rivers, to generate their own personal electricity. As the electrical grid developed, it became more economical and efficient to produce electricity in massive central locations and to distribute the electricity to customers as a utility. This freed up corporations to focus on their core missions, without the encumbrance of managing their own electrical generating plant.

Similarly, software, hardware, and data may be provided as a central utility, supplying customers at low cost. This would liberate individuals and corporations to focus on their core missions, rather than maintaining an information technology department, dealing with security, applying updates and patches, managing a ‘help desk’, etc.v

With our nation’s cyber landscape destined to change, and cyberterrorism evolving its target of attack, we must channel our thoughts and actions toward the future of both cyberterrorism and technology; we must understand their convergence, and we must address the security requirements of that future.

Regardless of whether cyberterrorism is a misnomer, a serious threat to life, safety, and our critical infrastructures, or just an annoyance, we need to be ever vigilant and forward-thinking to meet future challenges regarding cybersecurity.

Members of the Bureau

Members of the Bureau include federal IT security experts from government and industry. Bureau member, John R. Rossi, was the lead author of this peer-reviewed article. For a full list of Bureau members, visit www.isc2.org/ewb-usgov.

References:

Janczewski, L. & Colarik, A. (2008). “Cyber Warfare and Cyber Terrorism”. Page xiii. Information Science Reference, Hershey – New York

Ozeren, S. (2008). “Responses to Cyber Terrorism” page 70. Edited by Centre of Excellence Defense Against Terrorism, Ankara, Turkey. IOS Press.

Lachow, I. (2009). “Chapter 19: Cyber Terrorism: Menace or Myth?”

http://www.telegraph.co.uk/comment/personal-view/3640255/Cyber-terrorism-is-real---ask-Estonia.html

Carr, N. (2008). “The Big Switch”. W. W. Norton & Co.