'Code Wars: Steganography, Signals Intelligence, and Terrorism.' *Knowledge, Technology and Policy* (Special issue entitled 'Technology and Terrorism') Vol. 16, No. 2 (Summer 2003): 45-62 and reprinted in David Clarke (Ed.), *Technology and Terrorism*. New Jersey: Transaction Publishers (2004): 171-191.

Code Wars:
Steganography, Signals Intelligence, and Terrorism

Maura Conway

Department of Political Science
1, College Green
Trinity College
Dublin 2
Ireland

Tel. +353 1 608 3225
conwaym@tcd.ie

Author Bio Maura Conway is a PhD candidate in the Department of Political Science at Trinity College Dublin, Ireland, and a teaching fellow at the University of St. Andrews, Scotland. Her research interests are in the area of terrorism and the Internet. She has published in *Current History*, the *Journal of Information Warfare*, and elsewhere. Her research has been facilitated by a grant from the Irish Research Council for the Humanities and Social Sciences.

Abstract This paper describes and discusses the process of secret communication known as steganography. The argument advanced here is that terrorists are unlikely to be employing digital steganography to facilitate secret intra-group communication as has been claimed. This is because terrorist use of digital steganography is both technically and operationally implausible. The position adopted in this paper is that terrorists are likely to employ low-tech steganography such as semagrams and null ciphers instead.

Introduction

In 'A Few Words on Secret Writing' (1841), Edgar Allen Poe writes that "we can scarcely imagine a time when there did not exist a necessity, or at least a desire, of transmitting information from one individual to another in such a manner as to elude general comprehension" (as quoted in Rosenheim 1997, 171). Today, only a relatively small number of people worldwide employ strong security in their personal communications. However, an increasing amount of our social, economic, and work lives are conducted electronically - through e-mail, Net postings, electronic banking, e-commerce, etc. - and this has led to an increasing interest in questions of cybersecurity and online privacy, and pushed the issue of secret writing to the fore.

Perhaps when you were a child you used lemon juice to write on paper then allowed the paper to dry, which resulted in the disappearance of your text. Your writing would magically reappear on the apparently blank sheet of paper when you heated it. This is an example of steganography: the science of secret writing or the art of hiding messages within other messages.

"Steganography…has until recently been the poor cousin of cryptography" (Sellars 1999, 1). Although steganography is related to cryptography, they are not the same. The goal of steganography is to hide the existence of a message; the goal of cryptography is to scramble a message so that it cannot be understood, although its existence may be detected (Karp 2002). The advantage of steganography over cryptography is that it can be employed to secretly transmit messages without the fact of the transmission being discovered. In fact, it is common for steganographers to encrypt their hidden message before placing it in the cover message, although it should be noted that the hidden message does not have to be encrypted to qualify as steganography. A message can be in plain English (or any other language for that matter) and still constitute a hidden message. Nonetheless, those that employ steganography in their communications are generally careful to make use of the extra layer of protection that encryption provides. This is because covert information is not necessarily secure, just as secure information is not necessarily covert (Cochran 2000, 15).

Steganography hit the headlines when, between February and July 2000, *USA Today* reported that terrorists were using steganography to hide their communications from law enforcement agencies. According to the articles' author, Jack Kelley, the messages were being hidden in images posted on the Internet. Kelley gave the example of images posted on the Internet auction site eBay. There was very little evidence to substantiate these claims provided in the newspaper articles; nonetheless, in the wake of 9/11, media outlets worldwide picked up the story. This paper explores the plausibility of the claims made by Kelley in his articles. The paper is divided into five sections. Section one details the historical background to steganography, while section two outlines some of the technical details pertaining to digital steganography. The third section describes the alleged use of steganography by terrorists as reported in newspapers and magazines. In section four, I describe and discuss the process of steganalysis – the science of detecting hidden messages – one of the reasons why terrorists might be unwise to use steganography to conceal their communications. Finally, section five is devoted to an analysis of what alternative methods of clandestine communication via the Internet terrorists might employ instead. The argument advanced here is that terrorists are unlikely to be employing digital steganography to facilitate secret intra-group communication as Kelley and others have claimed. This is because terrorist use of digital steganography is both technically and operationally implausible. The position adopted in this article is that terrorists are likely to employ low-tech steganography such as semagrams and null ciphers instead.

A Brief History of Steganography

Steganography means covered or secret writing in Greek.[1] It is a form of information-hiding that has a long and established pedigree. The earliest known examples of steganography were recorded by the Greek historian Herodotus and date back to ancient times. The Greek tyrant Histaeus was held prisoner by King Darius in Susa during the 5th century BCE. Histaeus wanted to send a message to his son-in-law Aristagoras in Miletus, so he shaved the head of a slave and tattooed a message on his scalp. When the slave's hair grew long enough to conceal the message/tattoo, he was dispatched to Miletus (Byte 1997/8).[2] Herodotus provides us with another example of steganography from antiquity: the Greeks often communicated by writing on wax-covered tablets; when the Greek, Demeratus, needed to secretly notify the Spartans that Xerxes intended to invade Greece, he scraped the wax off of a tablet and wrote the message on the wood underneath. He then recovered the wooden tablets with wax. On inspection, the tablets appeared blank and unused, thus ensuring that Demeratuses message remained undiscovered (Cochran 2000, 12; Sellars 1999, 4).

Invisible inks are not simply children's playthings; they have been a popular method of chemical steganography for centuries. The ancient Romans would write between the lines of a text using invisible inks concocted from such readily available substances as fruit juices, urine, and milk. In fact, invisible inks were used in military conflict as recently as World War II (Byte 1997/8; Sellars 1999, 4).

Gaspari Schotti was the author of the earliest book on steganography. His four hundred-page tome, entitled *Schola Steganographica*, was published in 1665. Schotti drew extensively upon the work of Johannes Trithemius (1462-1526), a German monk and early researcher in steganography and cryptography. Steganographic research continued to develop in the fifteenth and sixteenth centuries. Bishop John Wilkins - later the master of Trinity College, Cambridge - devised a number of steganographic processes that ranged from coding messages in sheet music and string knots to invisible inks. Auguste Kerckhoff's *Cryptographie Militaire* appeared in 1883 and was followed by Charles Briquet's *Les Filigraines* (1907), a historical dictionary of watermarks (Cochran 2000, 11-12; Sellars 1999, 4-5).

It was during the twentieth century that steganography came into it's own, however. The British employed Lord Robert Baden-Powell, the founder of the Boy Scout movement, as a scout during the Boer War (1899-1902). His job was to record the location of Boer artillery positions. To avoid suspicion were he captured, Baden-Powell worked his maps into drawings of butterflies. On casual inspection the drawings appeared innocuous; however, certain markings on the wings actually indicated the positions of enemy installations. World War II ushered in a period of intense research and experimentation in steganography and associated fields. Invisible inks were employed in the early war years; later, null ciphers (i.e. unencrypted messages) were used to convey secret messages. The null cipher, which had the appearance of an innocent message about everyday occurrences, was thought unlikely to arouse suspicion and therefore to be less prone to interception. Duncan Sellars gives the example of the following message sent by a German spy during WWII:

> Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

Decoding this message (by lifting the second letter in each word) reveals the following secret text: Pershing sails from New York June 1 (Johnson 1995; Sellars 1999, 5-6). Documents layout was also used to conceal secret information: by modulating the position of lines[3] and words,[4] messages could be marked and identified. In addition, techniques such as writing messages in typewriter correction ribbon, and using pin punctures to mark selected letters were also popular (Sellars 1999, 6; Stallings 1998, 27).

J. Edgar Hoover, the director of the FBI, dubbed the German invention of the microdot "the enemy's masterpiece of espionage" (Dembart 2001). Microdots are photographs reduced to the size of a period, which have the clarity of standard sized typewritten pages. Using microdots, secret messages could be photographically reduced and affixed as the dot for the letter 'i' or other punctuation on any document containing text. Microdots permitted the secret transmission of large amounts of data, including technical drawings and photographs. The existence of the micro-dot was discovered by the Allies in 1941 on a typed envelope carried by a German agent. At that time, fears about the transmission of secret messages were so intense that, in the United States, the international mailing of postal chess games, knitting instructions, newspaper clippings, and children's drawings were banned. It was also illegal to send cables requiring that specific types of flowers be delivered on a specific date, and eventually the US and British governments banned international flower deliveries altogether (Byte 1997/8; Johnson 1995; Sellars 1999, 6).

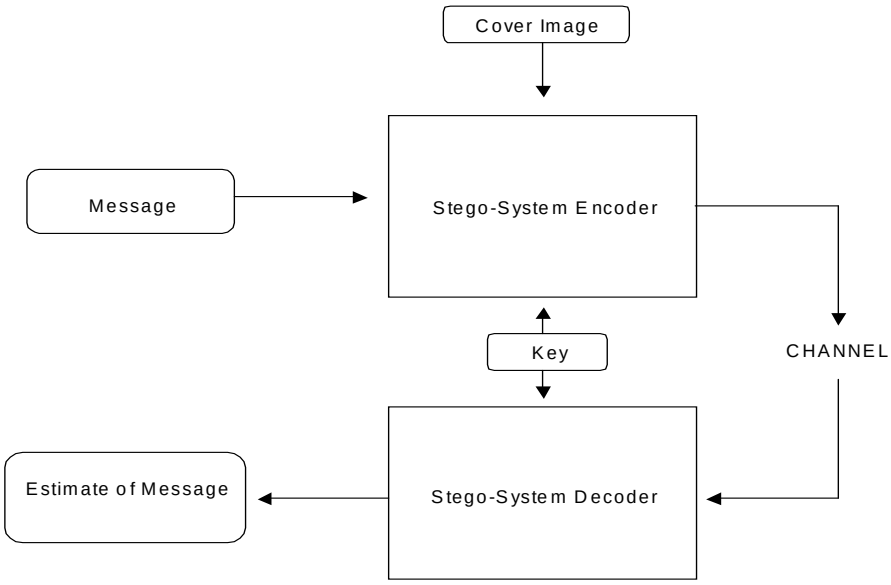
During the 1980s, the then-British Prime Minister Margaret Thatcher became so angered at press leaks of cabinet documents that she had the word processors in Westminster programmed to encode ministers' identities in the word spacing, so that those responsible for leaks could be identified (Anderson 1996, 39-40; Anderson & Petitcolas 1998, 474). More recently, the digital age has revolutionised steganography. In fact, according to some, the Internet has become the modern version of the 'dead drop,' a slang term describing the location where Cold War-era spies left maps, pictures, and other information, for collection by their handlers (Denning & Baugh 2001, 133; Kelley 2001a & 2001b).

Digital Steganography

The classic model for invisible communication in the modern scientific literature has been traced to G.J. Simmon, who in 1983 formulated it as the "Prisoners Problem." The scenario is this: Alice and Bob[5] are in jail, and wish to concoct an escape plan. However, all their communications pass through the warden, Willie; and if Willie detects any encrypted messages, he will negate their plan by restricting them to solitary confinement. The upshot of this is that Alice and Bob must find some way of hiding their ciphertext in an innocent-looking covertext; they must establish a subliminal channel, in other words (Anderson 1996, 39; Anderson & Petitcolas 1998, 474; Katzenbeisser 2000, 17-19). Alice could, for example, create a picture of a purple horse grazing in a red meadow and send this piece of modern art to Bob. If successful, Willie will have no idea that the colours of the objects in the drawing transmit information.

Computer-based (i.e. digital) steganography is a relatively new process. Its usefulness is based on two simple principles. The first is that the files that contain digitized images or sounds may be subtly altered without compromising their functionality. The second principle rests on

the inability of minor changes in colour or sound quality to be distinguished by humans (Johnson



& Jajodia 1998, 273). Digital steganography is usually based on randomness. There are many

Figure 1. Overview of Generic Steganographic Scheme[6]

occurrences of randomness in computer-based information. Steganographic data can be hidden in this random information or noise. The merits of a steganographic method are judged on whether the addition of the steganographic data changes the randomness (Ballard *et al* 2002, 996; Davern & Scott 1996, 279).

Digital steganography schemes can be characterised using theories of communication. The parameters of information hiding, such as the amount of data bits that can be hidden, the perceptibility of the message, and its robustness to removal can be related to the characteristics of communications systems: capacity, signal-to-noise ratio (SNR), and jamming margin. The notion of capacity in digital steganography indicates the total number of bits hidden and successfully recovered by the stego-system. The SNR serves as a measure of detectability. In this context, the message one is seeking to conceal (i.e. the embedded signal) represents the information-bearing signal, and the cover image is viewed as noise. Contrary to typical communication scenarios where a high SNR is desired, a very low SNR for a stego-system corresponds to lower perceptibility and therefore greater success when concealing the embedded signal. The measure of jamming resistance describes the level of robustness to removal or destruction of the embedded message, whether intentional or accidental (Marvel *et al* 1998, 48).

All digital steganographic schemes/tools employ the same basic principles. Let's assume that one wishes to hide a secret message in an image: the message is embedded in a digital image by the stego-system encoder, which uses a key or password, the resulting stego-image is transmitted in some fashion over a channel (e.g. the Internet) to an intended recipient, where it is processed by the stego-system decoder using the same key (see Figure 1).[7] During transmission, unintended or hostile viewers may monitor the stego-image, but they should observe only the transmittal of the innocuous image without discovering the existence of the hidden message (Ballard *et al* 2002, 998; Katzenbeisser 2000, 18-19; Marvel *et al* 1998, 49).

The possible covers for hidden messages are innocent looking carriers; in terms of digital steganography, these will be images, audio, video, text, or some other digitally representative code, which will hold or cover the hidden information. A message is the information hidden and may be plaintext, ciphertext, images or anything that can be embedded into a bit stream. Together the cover carrier and the embedded message create a stego-carrier. Hiding information may require a stego-key, which is additional secret information (e.g. a password) required for embedding the information. When a secret message is hidden within a cover image, the resulting product is a stego-image (Johnson & Jajodia 1998, 275). According to Mercer *et al*, to be useful, a steganographic system/tool must provide a method to:

(a.) Embed data invisibly,
(b.) Allow the data to be readily extracted,
(c.) Promote a high information rate or capacity, and
(d.) Incorporate a certain amount of robustness to removal (Mercer *et al* 1998, 49).

The remainder of this section is concerned with data encoding in still digital images. This is because the media attention surrounding terrorist use of steganography has focused on the latter.

Image steganography has made great strides in recent times with the development of fast, powerful graphical computers. Images provide excellent carriers for hidden information and many different techniques and tools have been developed for just this purpose.[8] These can be categorised into two groups: those in the Image Domain and those in the Transform Domain. *Image domain* tools encompass bit-wise methods that apply least significant bit (LSB) insertion and noise manipulation. These approaches are common in steganography and may be characterised as 'simple systems.' Typically, the image formats used in such steganography methods are lossless and the data can be directly manipulated and recovered. The *transform domain* grouping of tools include those that involve manipulation of algorithms and image transforms such as Discrete Cosine Transformation (DCT) and wavelet transformation. These methods hide messages in more significant areas of the cover and may manipulate image properties (e.g. luminance). These techniques are generally far more robust than bit-wise techniques. However, a trade-off exists between the amount of information added to the image and the robustness obtained. JPEG images use the DCT to achieve image compression (Johnson & Jajodia 1998, 276-277; see also Sellars 1999, 9-13 & Wayner 1996, Ch. 9).

There are a large number of stego-tools freely available on the Internet: Neil Provos' OutGuess is a universal steganographic tool that allows the insertion of hidden information into the redundant bits of data sources. It is freely available for download from http://www.outguess.org/. Another freely available steganography tool is Spammimic, which is available for download from http://www.spammimic.com: this site, developed by *Disappearing Cryptography* (1996) author Peter Wayner, gives you access to a program that will encrypt a short message into spam. Similarly, a program known as Snow hides information by adding extra white space at the end of each line of a text file or e-mail message. Steghide embeds messages in .bmp, .wav, and .au files, while MP3Stego does the same for MP3 files (McCullagh 2001a). And they are surprisingly easy to use (see Karp 2002):

> Basically, all a terrorist needs to do is choose a tool, 'stego' a message, and e-mail the message to a friend or post it to a publicly available site. Thereafter, an accomplice can retrieve this container message using the correct pass-phrase and the same software. Because steganography is not widely known, and technologically viable images are

> prolific on the Internet, it is very likely that the result image will go unnoticed as it reaches its destination (Ballard et al 2002, 998).

It is precisely this ease-of-use that has led many people to view steganography as an ideal terrorist tool.

Steganography Hits the Headlines

On 5 February 2001, an article penned by Jack Kelley and headlined 'Terrorist instructions hidden online' appeared in *USA Today*. In the article, Kelley claimed that:

> Through weeks of interviews with US law-enforcement officials and experts, *USA Today* has learned new details of how extremists hide maps and photographs of terrorist targets - and post instructions for terrorist activities - on sports chat rooms, pornographic bulletin boards and other popular Web sites…Officials and experts say the messages are scrambled using free encryption programs set up by groups that advocate privacy on the Internet. Those same programs can also hide maps and photographs in an existing image on selected Web sites. The e-mails and images can only be decrypted using a 'private key' or code, selected by the recipient.

Kelley goes on to quote Ben Venzke, special projects director for iDefense, a cyberintelligence company:

> The operational details and future targets, in many cases, are hidden in plain view on the Internet…Only the members of the terrorist organisations, knowing the hidden signals, are able to extract the information.

The evidence? A quote from CIA Director George Tenet:

> To a greater and greater degree, terrorist groups, including Hezbollah, Hamas, and bin Laden's al Qaida group, are using computerised files, e-mail, and encryption to support their operations.[9]

The next day, 6 February, Kelley followed up with 'Terror groups hide behind Web encryption:'

> Hidden in the X-rated pictures on several pornographic Web sites and the posted comments on sports chat rooms may lie the encrypted blueprints of the next terrorist attack against the United States or its allies.

The evidence? A quote from the FBI Director, Louis J. Freeh:

> Uncrackable encryption is allowing terrorists - Hamas, Hezbollah, al Qaida and others - to communicate about their criminal intentions without fear of outside

> intrusion…They're thwarting the efforts of law enforcement to detect, prevent and investigate illegal activities.[10]

Six months later, in July 2001, Kelley penned an article entitled 'Militants wire Web with links to jihad.' According to Kelley

> Muslim groups are increasingly turning to the Internet to carry on their jihad, or holy war, against the West…The groups use Web sites to plan attacks, recruit members and solicit donations with little or no chance of being caught by the FBI or other law enforcement agencies…Most of the information on the Web sites is written in Arabic and encrypted, or scrambled. The encrypted data is then hidden in digital photographs, which makes it difficult, if not impossible, to find or read…The groups regularly change the addresses of their Web sites to confound officials.

It is in this article that Kelley charges that al-Qaeda operatives have sent "hundreds of encrypted messages that have been hidden in files on digital photographs on the auction site eBay.com." This article also contains the first use of the term steganography by Kelley. According to the article

> US officials say that azzam.com contains encrypted messages in its pictures and texts - a practice known as steganography. They say the hidden messages contain instructions for al-Qaeda's next terrorist attacks. Mathematicians and other experts at the National Security agency at Fort Meade, Md., are using supercomputers to try to break the encryption codes and thwart the attacks.

The remainder of the article details the (freely available) contents of a number of Islamist Web sites.

Approximately three months later, shortly after the attacks of 9/11, the ABC News show *Primetime* dutifully revived the rumour, essentially claiming that it had been substantiated, though no evidence was produced. A stegged photo was produced, but it was a demo, not in any way associated with terrorism (see Ross 2001). Shortly afterwards an Associated Press article entitled 'Bin Laden's cybertrail proves elusive' appeared in *USA Today*. This article comes to rather different conclusions than those reached by Kelley and the producers at ABC. It's opening line reads

> Despite warnings from top government officials that terrorists would use exotic technology to communicate, suspected terrorist mastermind Osama bin Laden instead has used 'no-tech' methods, foiling efforts to track him, former US intelligence officials said.

In fact, according to this article, "Bin Laden relies on human messengers, safe houses and close-knit groups such as family members to send out his directives." Wayne Madsen, a former communications specialist for the National Security Agency, is quoted as saying, "This isn't low tech. You'd have to really call, it no-tech." In contrast to Bin Laden, Madsen admits that the 9/11 hijackers might have communicated via the Internet. He points to their possible use of seemingly innocuous messages posted on Web sites. For example, some minor change to a Web site might indicate the launch date of an attack, because they knew it in advance (see below).

The above notwithstanding, Kelley's original allegations were picked up by *Time Magazine*. Adam Cohen, in his article 'When Terror Hides Online,' suggested that

> A terrorist mastermind could insert plans for blowing up a nuclear reactor in, say, the nose of a puppy on a pet-adoption website. Operatives in the field, told which nose to look at, could then check for their marching orders. Steganography is a fast, cheap, safe way of delivering murderous instructions (Cohen 2001).

Cohen suggests that bin Laden's followers may have learned of steganography "when it burst on the pop-culture scene in recent movies like *Along Came a Spider*." Controversy arose about Cohen's article when Matthew Devost of the Terrorism Research Center charged that the writer had misrepresented him. It appears from the article that Devost believes that terrorists are using steganography on the Internet, but according to Devost: "I do not think that terrorists are using steganography on the Internet and I articulated this belief very clearly to Mr. Cohen."[11]

Finally, in October 2001, an article composed by Reuter's staff, entitled 'Researchers: No secret bin Laden messages on sites,' appeared in *USA Today*. That short piece detailed how computer science researchers at the University of Michigan had written a program to detect messages hidden inside photos on the Web. Peter Honeyman, scientific director of the University's Center for Information Technology Integration, and graduate student Neils Provost, ran a cluster of workstations against more than 2 million images on popular Web sites such as eBay, and attacked the candidates with a dictionary of more than 1.8 million words. They were prompted to do so by Kelley's original series of articles alleging that terrorists hide secret messages inside innocent-looking photos on the Web. They found nothing (see Provos & Honeyman 2001; also Manjoo 2001). This has not stopped some in the media pointing to terrorist use of steganography as a proven fact (see Friedman 2002; Lyman 2001; McGrory 2001, 11; Soloway, Nordland, Nadeau 2002), the most recent example being a headline in the *New York Post* which read '9/11 Plot Hidden in E-Porn' (Lathem 2003). Others are scathing; Ross Anderson of Cambridge University, an expert in Information Hiding, wrote a letter to *The Times* of London in which he questioned the motives of those "propagating this lurid urban myth."

> Perhaps the goal is to manufacture an excuse for the failure to anticipate the events of September 11th. Perhaps it is preparing the ground for an attempt at bureaucratic empire-building via Internet regulation, as a diversionary activity from the much harder and less pleasant task of going after al-Qaida. Perhaps the vision of bin Laden as cryptic pornographer is being spun to create a subconscious link, in the public mind, with the scare stories about child pornography that were used before September 11th to justify government plans for greater Internet regulation (Anderson 2001).

This is an argument put forward by a number of commentators as the reason for the widespread take-up of the allegations contained in Kelley's series of articles (see Leyden 2001 & Rosenheim 1997, 170). This is not the position explored here, however. Instead, the argument here is that terrorist use of digital steganography is both operationally unnecessary and technically risky.

Steganalysis

Steganalysis makes terrorist use of steganography technically risky. Steganalysis is the science of detecting hidden messages and thence the science of detecting steganography. Just as a cryptanalyst applies cryptanalysis in an attempt to decode or crack encrypted messages, the steganalyst is one who applies steganalysis in an attempt to detect the existence of hidden information (Johnson 2000, 80-81; Johnson & Jajodia 1998, 275). In cryptanalysis, portions of the plaintext (if it is available) and portions of the ciphertext are analysed. In steganalysis, comparisons are made between the cover object, the stego-object, and possible portions of the message. In cryptography, the end result is the ciphertext; in steganography, the end result is the stego-object. With steganography, the hidden message may or may not be encrypted, as noted earlier. If it is encrypted, then cryptanalysis techniques may be applied to further understand the embedded message on its extraction (Johnson 2000, 81).

Different tools vary in their approaches for hiding information. Without knowing which tool has been employed and which, if any, stego-key has been used, detecting the hidden information may become quite complex. However, some of the tools produce stego-images with characteristics that act as signatures for the steganography method or tool used (Johnson 2000, 80; Johnson & Jajodia 1998, 277). It has always been theoretically possible to produce a completely unbreakable code or completely secret channel, but only at considerable inconvenience. Steganography is not foolproof.

There are two methods of attack on steganography: detection of the embedded message and destruction of the embedded message. Clearly detection defeats the goal of steganography, which is to hide the existence of an embedded message. Destruction advances a step further and prevents the intended recipient of the message from accessing the information contained therein.

Digital images provide excellent covers for hidden information. However, distortions may occur as a result of embedding information. Selecting the optimum combination of steganography tools and covers is key to successful information hiding. Images can become grossly degraded with even small amounts of embedded information. This ‘perceptible noise’ can advertise the existence of hidden information. Characteristics of digital images that point to the existence of hidden information include unusual sorting of colour palettes, relationships between colours in colour indexes, or exaggerated ‘noise.’ One approach to identifying such patterns is to compare the original cover images with the stego-images and note visible differences. Minute differences are readily noticeable when comparing the cover and stego-images (Johnson 2000, 82). Ross Anderson dismisses most commonly used steganography tools as providing inadequate security. According to Anderson, there are three or four generations of Steganography software available; however, “The stuff you can download is first generation and easily defeated” (McCullagh 2001b).

Neil Johnson, whose work has been utilised extensively in this paper, is currently associate director of George Mason University’s Centre for Secure Information Systems. He is one of a small but growing number of digital detectives working in the field of steganalysis. According to Johnson, his techniques recently helped police to take into custody a suspect who raised suspicions after repeatedly e-mailing innocuous photographs to addresses that appeared to be of family members, without ever receiving any replies. "I identified the stego signature that law enforcement used to catch the guy," said Johnson. The US National Security Agency (NSA) and police agencies have underwritten Johnson’s research. In fact, the NSA certifies his centre’s graduate program at George Mason, and the Pentagon funds related research at other institutions.

The United States military also maintains a keen interest in research into new steganography software and applications and the development of new steganalysis tools. The

Naval Research Laboratory and the United States Air Force have been parties to the fourth and fifth annual Information Hiding Workshops, which took place in Pittsburgh in 2001 and in the Netherlands in 2002 respectively. WetStone technologies based in New York state have also made progress in a tool to detect steganography. Their *Steganography Detection and Recovery Toolkit* is being developed for the US Air Force Research Laboratory in Rome, New York. The goal of the toolkit is "to develop a set of statistical tests capable of detecting secret messages in computer files and electronic transmissions, as well as attempting to identify the underlying steganographic method." The project arose out of a study the Air Force commissioned from WetStone on forensic information warfare in 1998. At that time, the company was asked to identify technologies that the Air Force needed to guard against and it highlighted steganography as one of these (McCullagh 2001b).

Lastly, any cover can be manipulated with the goal of disabling or destroying some hidden information, whether there is an embedded message contained therein or not. While detecting the existence of a hidden message will save time in the disabling phase by processing only those covers that contain hidden information, detection is not a bar to disablement. Consider the scenario mooted by Kelley in his July 2001 article: an individual wishes to covertly communicate by hiding messages in images on public Internet sites. Suppose all image files uploaded by this individual, say Alice, pass through some gateway, perhaps a computer server, which is under the control of Bob. Bob wants to automatically introduce noise into *all* image files passing through the gateway in order to disrupt any such covert communication. Bob need not examine the files individually to try to find hidden information. Rather, the disruption may be completely automated (Ettinger 1998, 321). So, reverting to Kelley's assertion that terrorists are hiding instructions for attacks on sites such as eBay and, presuming that this were actually taking place, eBay and other similar sites would have at their disposal a fairly simple means of stamping out such practices. So why not employ low-tech steganographic methods instead?

Low-Tech Steg

There is ample evidence supporting the assertion that terrorists employ encryption on files stored on their computer's hard drives and in their electronic communications. According to Denning and Baugh, some terrorist groups are employing high-frequency encrypted voice and data links to communicate with their state sponsors. They also state that Hamas is using encrypted Internet communications to transmit maps, pictures, and other details pertaining to terrorist attacks[12] (Denning & Baugh 2001, 117; see also Jolish 2002). The FBI located encrypted files on the laptop computer of Ramsey Yousef, a member of the group responsible for the original attack on the World Trade Centre in 1994 and a Philippine airliner in late 1995. On decryption these files were found to contain information detailing further plans to blow up eleven US-owned commercial airliners in the Far East. Much of this information was also available in unencrypted documents, but successful decryption of electronic records can be important to an investigation. This was the case when Japanese authorities seized the computers of the Aum Shinrikyo cult. Aum was the group responsible for releasing sarin gas in the Tokyo subway in March 1995, which resulted in the deaths of 12 people and injured 6,000 more. Aum had stored encrypted information on the computers; the authorities were able to decrypt the files after the finding the key on a floppy disk. According to Denning and Baugh, the files contained evidence that was crucial to the investigation (Denning & Baugh 2001, 120).

There have been a small number of reported cases of criminals using steganography to facilitate their crimes. For example, a credit card thief used it to hide stolen card numbers on a hacked Web page. He replaced bullets on the page with images that appeared the same, but that contained the credit card numbers, which he then offered to associates (Denning & Baugh 2001, 133). There is no substantiated evidence of terrorists employing the same techniques, however. A majority of the media accounts detailing terrorist use of steganography draw heavily on the original unsubstantiated assertions made by Jack Kelley in *USA Today*. It has become an article of faith that bin Laden and his associates routinely communicate through stegged messages posted on pornographic Web sites.[13] The following statement by US Army Lt. Gen. Joseph Kellogg Jr., Director of Command, Control, Communications, and Computers for the Joint Staff, is fairly representative: "They are hiding stuff in pictures and embedding them in places we can't get to…like porn sites" (Caterinicchia 2003). Which raises the question, if you cannot get to them, how you know they're there? By reading *USA Today* perhaps?

There are those who are sceptical of these assertions, however. Indeed, many analysts believe that al-Qaeda uses prearranged phrases and symbols (i.e. low-tech steganography) and not digital steganography to direct its operatives. With regard to the Internet for example, "an icon of an AK-47 can appear next to a photo of Osama bin Laden facing one direction one day, and another the next. Colours of icons can change as well. Messages can be hidden on pages inside sites with no links to them, or placed openly in chat rooms" (Soloway *et al* 2002). Secret communications of this type (i.e. those that are not in written form) are known as semagrams. Similar forms of communication have proved successful in the past. In 1993, for example, the forces of Somali warlord Mohamed Farah Aidid banged out messages on drums instead of using telephones in order to thwart the efforts of US forces seeking to intercept his communications.

In the 1980s, David O'Connell, the then-Chief of Staff of the Provisional Irish Republican Army (PIRA), gave a television interview in which he announced the commencement of a bombing campaign in Britain, which materialised a week later with the bombing of two bars in Birmingham in which 21 people died. The possibility exists, although it cannot be proven, that O'Connell used the television appearance to signal the attacks to PIRA operatives stationed in the UK (Schmid & De Graaf 1982, 43). It was probably similar fears that prompted US National Security Adviser, Condoleeza Rice, to request US television networks not to air the video of Osama bin Laden that was delivered to Al Jazeera television in the wake of 9/11. The US networks declined the request due, they said, to the fact that the video was easily downloadable via the Internet and therefore already freely available. In February of this year, George Tenet, the director of the CIA, told the Senate Armed Services Committee, that analysts were examining audio recordings allegedly made by Osama bin Laden, looking for particular phrases or words that might be coded signals to al-Qaeda operatives in the field. In particular, analysts were said to be examining passages of audio that referred repeatedly to al-Qaeda's efforts to dig "trenches" in Afghanistan and statements urging his followers to "fight in the plains, mountains, farms, and cities." An individual described as a "senior intelligence official" said that analysts had not come to any definitive conclusions, but said that it was possible that the message, taken in its entirety, was a "go signal" (Johnston 2003).

In an interview recounted in London's *Sunday Times* newspaper, two of those involved in the preparations for the 9/11 attacks, Khalid Sheikh Mohammed and Ramzi Binalshibh, revealed to a reporter from Al Jazeera television that Mohammed Atta communicated with Binalshibh in German via the Internet. He posed as a student in America contacting his girlfriend 'Jenny' in Germany. According to Mohammed and Binalshibh, an elaborate code was agreed so that Atta

could keep in touch with his al-Qaeda commanders through e-mail and Internet chat rooms. For example, the targets were referred to as university departments: the Twin Towers were the 'faculty of town planning' - Atta's academic speciality; Capitol Hill was the 'faculty of law' and the Pentagon was the 'faculty of fine arts' (Fielding 2002, 1; Fouda 2002, 15-17). Yosri Fouda, the journalist who conducted the interview, reports that he saw the last communication between Atta and Binalshibh, which was conducted in German and took place in an Internet chat room. It read:

> "The first semester starts in three weeks. Nothing has changed. Everything is fine. There are good signs and encouraging ideas. Two high schools and two universities. Everything is going according to plan. This summer will surely be hot. I would like to talk to you about a few details. Nineteen certificates for private study and four exams. Regards to the professor. Goodbye" (Fouda 2002, 17).

A similar strategy was employed by anti-communist terror squads in El Salvador in 1977 when on election day they seized the radio station of the National Water Authority and used it to instruct their followers with coded messages. The code word for the opposition votes was 'coffee' and 'sugar' meant votes for the terror squad's own supporters. 'Little birds' were election supervisors and 'giving lessons' meant to intimidate them. 'Put some *Tamales* in the tank' signified filling ballot boxes with fraudulent votes. Those candidates who supported the right-wing terror squads triumphed in the radio-controlled election (Schmid & De Graaf 1982, 26-27).

Conclusion

The Internet and the abilities of intelligence officials to eavesdrop on e-mail and phone calls, was supposed to help prevent attacks such as those that occurred in New York and Washington from ever coming to successful fruition. In the event they did not and, as a result, assumptions about the role the Internet can play in fighting terrorism are being challenged. Investigators are nevertheless relying on Internet tools in their investigation as never before (Schwartz 2001). What role did the Internet played in the investigation of the attacks? Importantly, what could be done online to track the group depended in large part on what the group did online. In a briefing given in late September 2001, FBI Assistant Director Ronald Dick, then head of the US National Infrastructure Protection Center (NIPC), told reporters that the hijackers had used the Net, and "used it well."

US federal agents issued subpoenas and search warrants to just about every major Internet company, including America Online, Microsoft, Yahoo, Google, and many smaller providers. It is known that the hijackers booked at least nine of their airline tickets for the four doomed flights online at least two to three weeks prior to the attacks. They also used the Internet to find information about the aerial application of pesticides. Investigators are said to have in their possession hundreds of e-mails linked to the terrorists in English, Arabic and Urdu. The messages were sent within the US and internationally. According to the FBI, a number of these messages include operational details of the attacks. Some of the hijackers used e-mail services that are largely anonymous - Hotmail, for example - and created multiple temporary accounts. A number of them are known to have used public terminals, in libraries and elsewhere, to gain

access to the Net, whereas others used privately owned personal or laptop computers to do so (Cohen 2001; Fallis & Cha 2001, A24).

In two successive briefings, senior FBI officials stated that the agency had found no evidence that the hijackers used electronic encryption methods to communicate on the Internet. This has not, however, prevented politicians and journalists repeating lurid rumors that the coded orders for the attacks were secretly hidden inside pornographic web images, or from making claims that the attacks could have been prevented had Western governments been given the power to prevent Internet users from employing encryption in their communications[14] (Cha 2001). Although many e-mail messages sent to and from key members of the hijack teams have been uncovered and studied, none of them, according to the FBI, used steganography. Evidence from questioning terrorists involved in previous attacks, both in America and on American interests abroad, and monitoring their messages reveals that they simply used words to make their communications appear innocuous to eavesdroppers.

At base, steganography is a procedure for hiding information from an enemy's prying eyes and is therefore not a new idea, as illustrated in section one. Digital steganography is a relatively new invention however and section two is devoted to demystifying it. It has been widely reported – in *USA Today*, the *New York Times*, the *Times* of London, *Newsweek*, *Time* magazine, and many other venues – that terrorist groups employ digital steganography to engage in covert communication. In particular, the assertion that Islamist terrorist organizations routinely post secret information and plans on pornographic Web sites is accepted as fact. A large part of this article is concerned with showing that this is unlikely to be the case. The argument here is not that terrorists do not employ steganography, but that they are more likely to employ low-tech steg (e.g. null ciphers, semagrams, etc.) than high-tech steg (i.e. digital steganography tools) in their communications. This is because the use of digital steganography by such groups is both technically risky- due to the availability of tools to detect stegged messages - and operationally implausible – due to the availability of low-tech steganography methods the existence of which are difficult to detect and almost impossible to prove. To conclude: the main problem facing communications intelligence experts is selection (i.e. knowing which of the billions of e-mails or Web images to look at) rather then the possibility that the e-mails or images might be stegged, encrypted, or otherwise camouflaged. A competent opponent is unlikely to draw attention to himself by being one of the few users of digital steganography.

Endnotes

[1] Cryptography means 'secret writing.'

[2] Astonishingly, this method was still used by some German spies at the beginning of the twentieth century.

[3] This is known as line-shift coding. In this method, text lines are vertically shifted to encode the document uniquely. This method is probably the most visible text coding technique to the reader, however (see Sellars 1999, 7).

[4] This is known as word-shift coding. In this method, code words are included in a document by shifting the horizontal locations of words within text lines, while maintaining the appearance of natural spacing (see Sellars 1999, 8).

[5] In the field of cryptography, communication protocols usually involve two fictional characters named Alice and Bob. The standard convention is to name the participants in the protocol alphabetically (Carol and Dave often succeed Alice and Bob in a multi-person protocol), or with a name whose first character matches the first letter of their role (e.g. Willie the warden).
[6] Adapted from Marvel *et al* 1998, 50. See also Shin 2000, 19.
[7] The terminology employed here was decided upon at the First International Workshop on Information Hiding which was organized by Ross Anderson and took place at Cambridge University, UK, in 1996 (see Pfitzmann 1996, 347-350).
[8] To view examples of 'before' and 'after' images (i.e. an image containing a hidden message and the same image with no hidden data contained in it), see Johnson 1995; Marvel *et al* 1998, 58.
[9] From a document Tenet wrote to the US Senate Foreign Relations Committee in March 2001.
[10] Freeh's testimony was given during a closed-door hearing on terrorism before a Senate panel in March 2001.
[11] Devost's comments are posted on his Web site at http://www.devost.net/archives/000036.html.
[12] According to Denning and Baugh, the Israeli General Security Service believes that most of the data is being sent to the Hamas worldwide centre in Great Britain (2001, 117).
[13] The frequency of such assertions led one journalist to comment "that the likelihood of Islamic fundamentalists hiding messages in porn is roughly the same as their likelihood of hiding them in pig carcasses" (Greene 2003).
[14] In Britain, Foreign Secretary Jack Straw provoked a storm of protest by suggesting on the BBC that the media and civil liberties campaigners had paved the way for the terror attacks on America by advocating free speech and favoring publicly available encryption.

References

Anderson, Ross. 2001. 'Reply to the Times Article: Secrets Concealed by Software.' http://lists.jammed.com/crime/2001/10/0027.html.

Anderson, Ross & Fabien A.P. Petitcolas. 1998. 'On the Limits of Steganography.' *IEEE Journal of Selected Areas in Communication* 16(4): 474-481. http://www.cl.cam.ac.uk/~fapp2/publications/jsac98-limsteg.pdf.

Anderson, Ross. 1996. 'Stretching the Limits of Steganography.' *Lecture Notes in Computer Science* No. 1174, 39-48.

Andrew, Christopher. 2001. 'Counsel of War.' *The Times: T2* (London) 4 October, 2-3.

Associated Press. 2001. 'Bin Laden's Cybertrail Proves Elusive.' *USA Today* 20 September. http://www.usatoday.com/tech/news/2001/09/20/attacks-cybertrail.htm.

Ballard, James David, Joseph G. Hornik, & Douglas McKenzie. 2002. 'Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues.' *American Behavioral Scientist* 45(6), 989-1016.

Byte, Mr. 1997/8. *Privacy Guide*. http://www.all-nettools.com/privacy/.

Caterinicchia, Dan. 2003. 'Kellogg Describes Cyber Battlefield.' *Federal Computer Week* 5 March. http://www.fcw.com/fcw/articles/2003/0303/web-kellogg-03-05-03.asp.

Cha, Ariana Eunjung. 2001. 'To Attacks' Toll Add a Programmer's Grief.' *Washington Post* 21 September, p. E01.

Cochran, Jordon T. 2000. *Steganographic Computer Warfare*. Wright-Patterson Air Force Base, Ohio: Air Force Institute of Technology. http://www.iwar.org.uk/iwar/resources/usaf/maxwell/students/2000/afit-gcs-eng-00m-03.pdf.

Cohen, Adam. 2001. 'When Terror Hides Online.' *Time* 12 November.

Davern, Paul & Michael Scott. 1996. 'Fractal Based Image Steganography.' *Lecture Notes in Computer Science* No. 1174, 278-294.

Dembart, Lee. 2001. 'Hide Your Secrets: Old Art of Concealed Messages Rediscovered on the Internet.' *International Herald Tribune* 7 May.

Denning, Dorothy & William E. Baugh. 2001. 'Hiding Crimes in Cyberspace.' In Peter Ludlow (ed.), *Crypto Anarchy, Cyberstates, and Pirate Utopias*. Cambridge MA: MIT Press.

Ettinger, J. Mark. 1998. 'Steganalysis and Game Equilibria.' *Lecture Notes in Computer Science* No. 1525, 319-328.

Fallis, David S. & Ariana Eunjung Cha. 2001. 'Agents Following Suspects' Lengthy Electronic Trail.' *Washington Post* 4 October, p. A24.

Fielding, Nick. 2002. 'Leaders of Sept 11 Boast of US Attack.' *The Sunday Times* 8 September, p. 1.

Fouda, Yosri. 2002. 'The Masterminds.' *The Sunday Times* 8 September, 15-17.

Friedman, Thomas L. 2002. 'Webbed, Wired and Worried.' *The New York Times* 26 May. http://www.nytimes.com/2002/05/26/opinion/26FRIE.html.

Greene, Thomas C. 2003. 'Al-Qaeda Said to be Using Stegged Porn.' *The Register* (UK) 12 May. http://www.theregister.co.uk/content/55/30654.html.

Henderson, Mark. 2001. 'Secrets Concealed by Software.' *The Times* (London) 6 October, p. 11.

Johnson, Neil F. 2000. 'Steganalysis.' In Stefan Katzenbeisser & Fabien A. Petitcolas (ed.s), *Information Hiding: Techniques for Steganography and Digital Watermarking*. Boston & London: Artech House, 79-93.

Johnson, Neil. 1995. *Steganography*. Virginia: George Mason University. http://www.jjtc.com/stegdoc/steg1995.html.

Johnson, Neil F. & Sushil Jajodia. 1998. 'Steganalysis of Images Using Current Steganography Software.' *Lecture Notes in Computer Science* No. 1525, 273-289.

Johnston, David. 2003. 'Bin Laden Tape may Hint at Attack, CIA Says.' *The New York Times* 13 February.

Jolish, Barak. 2002. 'The Encrypted Jihad.' *Salon.com* 4 February. http://www.salon.com/tech/feature/2002/02/04/terror_encryption/.

Karp, Jack. 2002. 'A Novice Tries Steganography.' *Tech TV* 12 February. http://www.techtv.com/cybercrime/privacy/story/0,23008,3359041,00.html.

Katzenbeisser, Stefan C. 2000. 'Principles of Steganography.' In Stefan Katzenbeisser & Fabien A. Petitcolas (ed.s), *Information Hiding: Techniques for Steganography and Digital Watermarking*. Boston & London: Artech House, 17-41.

Kelley, Jack. 2001a. 'Terrorist Instructions Hidden Online.' *USA Today* 5 February. http://www.usatoday.com/tech/news/2001-02-05-binladen-side.htm.

Kelley, Jack. 2001b. 'Terror Groups Hide Behind Web Encryption.' *USA Today* 6 February. http://www.usatoday.com/tech/news/2001-02-05-binladen.htm.

Kelley, Jack. 2001c. 'Militants Wire Web with Links to Jihad.' *USA Today* 10 July. http://www.usatoday.com/news/world/2002/07/10/web-terror-cover.htm.

Lathem, Niles. 2003. '9/11 Plot Hidden in E-Porn.' *New York Post* 9 May. http://www.nypost.com/news/worldnews/57502.htm.

Leyden, John. 2001. 'Militants Plan Terror in Chat Rooms Shocker.' *The Register* (UK) 6 February. http://www.theregister.co.uk/content/archive/16684.html.

Lyman, Jay. 2001. 'How Terrorists Use the Internet.' *NewsFactor Network* 12 September. http://www.newsfactor.com/perl/story/7731.html.

Manjoo, Farhad. 2001. 'Hidden Messages: Any There?' *Wired* 8 November. http://www.wired.com/news/technology/0,1282,48235,00.html.

Marvel, Lisa M., Charles G. Boncelet, & Charles T. Retter. 1998. 'Reliable Blind Information Hiding for Images.' *Lecture Notes in Computer Science* No. 1525, 48-61.
McGrory, Daniel. 2001. 'Al-Qaeda Hid Coded Messages on Porn Websites.' *The Times* (London) 6 October, p. 11.

Pfitzmann, Birgit. 1996. 'Information Hiding Terminology.' *Lecture Notes in Computer Science* No. 1174, 17-28.

McCullagh, Declan. 2001a. 'Bin Laden: Steganography Master?' *Wired* 7 February. http://www.wired.com/news/politics/0,1283,41658,00.html.

McCullagh, Declan. 2001b. 'Secret Messages come in .Wavs.' *Wired* 20 February. http://www.wired.com/news/politics/0,1283,41861,00.html.

Provos, Neils & Peter Honeyman. 2001. *CITI Technical Report 01-11: Detecting Steganographic Content on the Internet*. University of Michigan: Center for Information Technology Integration. http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf.

Reuters. 2001. 'Researchers: No Secret bin Laden Messages on Sites.' *USA Today* 17 October. http://www.usatoday.com/tech/news/2001/10/17/bin-laden-site.htm.

Rosenheim, Shawn. 1997. *The Cryptographic Imagination: Secret Writing From Edgar Poe to the Internet*. Baltimore & London: Johns Hopkins University Press.

Ross, Brian. 2001. 'A Secret Language: Hijackers May Have Used Secret Internet Messaging Technique.' *ABC News* 4 October. http://abcnews.go.com/sections/primetime/DailyNews/PRIMETIME_011004_steganography.html.

Schmid, Alex P. & Janny De Graaf. 1982. *Violence as Communication: Insurgent Terrorism and the Western News Media*. London: Sage.

Schwartz, John. 2001. 'Securing the Lines of a Wired Nation.' *New York Times* 4 October.
Sellars, Duncan. 1999. *An Introduction to Steganography*. South Africa: University of Cape Town. http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html.

Shin, Natori. 2000. 'One-Time Hash Steganography.' *Lecture Notes in Computer Science* No. 1768, 17-28.

Soloway, Colin, Rod Nordland, & Barbie Nadeau. 2002. 'Hiding (and Seeking) Messages on the Web.' *Newsweek* 17 June. http://cert.uni-stuttgart.de/archive/isn/2002/06/msg00040.html.

Stallings, William. 1998. *Cryptography and Network Security: Principles and Practice*. New Jersey: Prentice Hall.

Wayner, Peter. 1996. *Disappearing Cryptography: Setting Up Networks with Hidden Communications*. Boston: AP Professional.