CYBER CRIME CHRONICLES

2ND EDITION

Virtual Wild West, Darkest Vices, Hackers, Victims
Living life on the Internet

They're all still down there, out of sight and all but out of mind --hundreds of millions of miles of hair-thin strands of glass, uniquely strung beneath the streets of every city, under our homes, suburbs, deserts, and strewn across the ocean floor. It's enough optical fibre to wrap around the earth 4,000 times (scary statistics), with each strand capable of blasting library stacks of information across the globe at the speed of light. And almost all of it sits empty, dark and idle -- an unseen monument to every unfulfilled promise of the Internet. A statistical reality people can't even begin to comprehend.

All the experts said we needed all of it and more because once we discovered the power of the World Wide Web; there would be no stopping it. Billions would flood into cyberspace, changing everything about the way we communicate, educate and entertain, and ultimately a force that changes and controls the very essence of our lives.

They're still selling the same old line. On Oct. 9, Google bought YouTube -- an Internet site used primarily for the unauthorized distribution of copyrighted material and minute-long clips of people singing karaoke in their basements. This titan of new media, we're told, is worth US$1.65 billion. It's just the latest step in our long descent into cyber-madness. After 15 years and a trillion dollars of corporate investment, just about everything we've been told about the Internet and what the information age would mean has come up short. The numbers will just get worse and more terrifying.

The idealists, engineers and programmers who conceived, pioneered, and engineered the Web described a kind of enlightened utopia built on mutual understanding, a world in which knowledge is limited only by one's curiosity. Instead, we have constructed a virtual Wild West, where the masses indulge their darkest vices, pirates of all kinds troll for victims, and the rest of us have come to accept that cyberspace isn't the kind of place you'd want to raise your kids. The great multinational exchange of ideas and goodwill has devolved into nothing more than cyber-terrorism. And the virtual marketplace is a great place to get robbed. The answers to the great questions of our world may be out there somewhere, but finding them will require you to first wade through an ocean of misinformation, trivia and human sludge. We have been sold a bill of good.

Let's put this in terms crude enough for all cyber-dwellers to grasp. The Internet is becoming a very dangerous medium that needs all aspects of divine and human intervention for us to stay stable.

Right from the beginning, experts competed with one another to see who could come up with the best form of technology and human intervening medium. This competition is far from being over. It was the most important breakthrough since the personal computer, no, since the telephone -- or rather the telegraph, or maybe the printing press. Bill Gates, in a famous editorial for the New York Times, called the Internet a "tidal wave" that "will wash over the computer industry and many others, drowning those who don't learn to swim in its waves." You are either with it or will drown in it, simplistically put.

But it was John Perry Barlow, former lyricist for the Grateful Dead turned Internet visionary and co-founder of the Electronic Frontier Foundation, who set the gold standard for sweaty-palmed exuberance back in 1995 when Harper's magazine asked him to take part in a four-person discussion on the future of the Web. "With the development of the Internet . . . we are in the middle of the most transforming technological event since the capture of fire," he said. What's perhaps most telling is not so much that Barlow would make such a monumental claim, but that nobody on the panel cracked up laughing, or even so much contested the claim.

We've tempered our rhetoric in recent years, but only slightly. This year, the National Academy of Engineering released its list of the 20 greatest engineering accomplishments of the past 100 years. The Internet ranked 13th, but even that ranking seems generous. For instance, it came in just ahead of imaging technologies like the X-ray, MRI and radar -- breakthroughs that have allowed us to look inside the human body without breaking the skin, to predict the weather, and to see things invisible to the human eye. Has the Internet achieved anything remotely comparable? Next on the list are household appliances. Try going back to doing the family's laundry by hand for one week, and then see if you'd gladly trade your Internet connection to get your washing machine back. There is a humorous and honest statement.

Robert Gordon, an economics professor at Northwestern University, is one of the few who've consistently argued that the Internet is a useful tool, but not a revolutionary one. The inherent trouble with the Net, he says, is that it has produced precious little that is really new. Just about everything that's accessible through the Web was available through other means before. Email is fine, for instance, but it pales next to the achievement of the telegraph, which shortened the time required to communicate over vast distances from weeks to minutes. The internal combustion engine, refrigeration, even air conditioning, had profound impacts on our lives, making the impossible practical. The Web does nothing of the sort. Emails have replaced faxes and phone calls. Online shopping replaces sales that used to be made through a catalogue. And, for all but the most socially isolated, every hour spent trolling through chat rooms replaces an hour that might otherwise have been spent in real, live one-on-one conversation.

Even in the research and academic communities, which always had the most to gain from the Internet, Gordon says, the advantages should be kept in perspective. "It has made collaboration and communication faster and more efficient, but we're still doing the same things," he says. "The great works in my field were all written before the Internet. It didn't make possible a great improvement in quality, it just made it possible to get things done more easily."

That's important, because if the Internet was only ever about convenience and finding quicker ways of doing the same old things, then all those lofty claims that drove the Internet into the mainstream were little more than an isolated hype. But, as history has shown many times, hype has proven to be a very lucrative and successful form of business.

In the late 1990s, just as the dot-com gold rush was reaching manic proportions, Jack Welch, chairman and CEO of General Electric and perhaps the most respected executive in the world at the time, described the Internet as "the Viagra of big business." Welch is known for his colourful analogies, but rarely did he hit the bull's eye so precisely as he did that day. Just like America's favourite little blue pill, the Internet produced in business a rush of extreme excitement, which temporarily interfered with normal brain function. It was manifested in one of the most impressive market climbs in modern history between 1998 and mid-2000 -- a euphoric ride, followed by an equally astonishing collapse. Like Viagra, it sure was fun while it lasted.

That much is well known. But what most people still don't realize is that much of the global Internet mania that transpired in the late 1990s was driven by a myth, willfully propagated by a handful of corporate executives, several of whom are now in prison. The magic number of the dot-com boom was that, between 1997 and 2000, Internet traffic was doubling every 100 days. It was a stunning statistic that seems to have begun with WorldCom Inc., the telecom company run by Canadian Bernie Ebbers, which collapsed amidst the scandal in 2002. That one statistic suggested the world was in the midst of a stampede to the Web, and it became one of the most immutable truths of the new economy, repeated in casual conversation by CEOs, analysts, day traders and taxi drivers. Whenever anyone would suggest that dot-com market valuations were getting out of hand, or pose a skeptical question, executives would simply pull out that jaw-dropping statistic.

According to professor Andrew Odlyzko of the University of Minnesota, Internet traffic was doubling every year between 1996 and 2002 -- still impressive, but a far cry from the more than 1,300 per cent annual growth implied by WorldCom officials and others. This was more than just an innocuous urban myth -- it was the seed of one of the most devastating and economically distorting episodes in modern history.

When the dot-com bubble finally burst in mid-2000, the losses ran into the trillions of dollars, and crushed the retirement dreams and career aspirations of millions. Where did all that money go? Some of it went to lay all that unused fibre optic cable. Some of it went to buy computer equipment for a thousand doomed Internet start-ups. And billions went to pay the bonuses of investment bankers and analysts, and to build vacation homes in the Caymans for the CEOs of dot-coms that no longer exist.

Google's purchase of YouTube suggests we're eagerly preparing to repeat our mistakes. MySpace, a money-losing social networking site, was similarly sold to NewsCorp almost a year ago for US$580 million. Speculation is now rampant. Yahoo! Inc. bought another nascent site, Facebook, for north of US$1 billion. All this for companies that did not exist a few years ago, and which have yet to prove that they can translate large traffic into even meager profits. Some analysts estimate YouTube is currently losing as much as US$1.5 million every month. One may ask why?

The Internet works like Viagra for big business, all right. But the list of those who get screwed goes far beyond just investors and pension plans.

In 1995, the U.S. government's top copyright officer, Marybeth Peters, called the Internet "the world's biggest copying machine." She didn't know the half of it. At the time, slow connection speeds and weak processing power meant the Web was still essentially a print medium. Within a couple of years, however, the full force of the Web's assault on intellectual property rights would come under the microscope and clearly into focus.

As we all remember, the real trouble commenced with Napster, the little company run by a 19-year-old named Shawn Fanning, who figured out a way to let users swap files stored on their hard drives over the Web. Within a year of its creation, Napster offered 200,000 songs available for free download. By February 2001, the site had more than 26 million users. The music industry sued for US$20 billion and eventually managed to put Napster out of the stolen-music business. But by the time the industry won, it had already lost. Napster was responsible for spawning dozens of copycat sites that continue to operate in the Web's legal grey zone, in which copying and distributing music and video for free is not really allowed, but isn't prevented either such as Limewire, Ares, Warez, etc.

The music industry partially solved the problem by giving in to it. All major record labels struck deals with legitimate online retailers like iTunes to make songs available for one dollar a track and albums for around $10. It won't stop most of the pirating, but at least now fans that are inclined to buy their music legitimately have a means to do so. At Christmas 2005, the burgeoning online music industry sold $20 million in digital music over the Web in a single week, and the popularity of such services continues to grow.

Still, illegal downloads from sites like Ares, Warez, Kazaa, Limewire, Acquisition and BitTorrent continue to outnumber legal ones by a significant margin. Music is now, for all intents and purposes, sold strictly on the honour system. And as connection speeds and computer storage capacity improve, the same is increasingly true for movies, television programs and sporting events. Despite the objections of major publishers, Google is pressing ahead with a project to scan and store digitized copies of millions of books that would be searchable on the Web. It will undoubtedly be an amazing research tool. It's also a potentially crippling blow to publishers whose businesses depend upon selling books to thousands of libraries around the world.

Some will undoubtedly find ways to make a virtue out of this new digital world. It will expose small artists to greater audiences than the old record company model. And it has already proven to be a ‘high' to consumers, who get almost unlimited choice and lower prices. But that benefit has arisen out of the fact that it has never been so easy and consequence-free to pilfer an exact copy of someone's work -- be it music, film, writing or research. To suggest the arts are ultimately better off thanks to Internet file sharing is to suggest that entertainers would've been better off to hand out CDs for free and live on donations from fans.

The whole system of ascribing an economic value to works of art has been thrown out the window. And artists aren't the only ones suffering from the sudden glut of cheap product being slung around the Web.

On Wednesday, July 5, Ken Lay, the former chairman and CEO of Enron Corp. died in Colorado. The news first hit the wires around 10 a.m., and at 10:06 Wikipedia, the online encyclopedia that allows users to update and modify entries, proclaimed that Lay had died "of an apparent suicide." Two minutes later, somebody changed the entry to say Lay had died "of an apparent heart attack or suicide." Less than a minute later, some cooler head intervened and corrected the entry to say the cause of death was "yet to be determined." At 10:11 the entry was changed again, this time asserting "The guilt of ruining so many lives finally led him to suicide." A minute after that, someone cited a news report that "according to Lay's pastor the cause was a 'massive coronary heart attack.' " Then, at 10:39, one of the Internet's anonymous, self-taught cardiologists wrote: "speculation as to the cause of the heart attack lead [sic] many people to believe it was due to the amount of stress put on him by the Enron trial." Finally, a few hours later, the entry was set straight, noting simply that Lay had died of a heart attack in Aspen. This example is a clear direction of how fast the internet is altering the truth of simple incidents but more importantly of “who” want to be on the top of the leading story. Don't be deceived by the speed of technology.

But other lies are not so easily set straight. Conspiracy theories, conjecture and outright fabrications masquerade as fact on the Internet, and often, nobody seems to notice the difference. The problem is rooted equally in the nature of humans and the nature of cyberspace. It does not dismiss the notion that facts must be supported and properly substantiated before being printed. The designers of the Internet put their deepest faith in the wisdom of the masses to establish truth and value by consensus. Google ranks search results based on how many others link to a particular site. Digg.com is a site organized according to users' ratings on what's interesting and what isn't. And Wikipedia, of course, is based upon the notion that hundreds of thousands of anonymous contributors, all acting as freelance fact checkers, can produce a reliable reference document. Unfortunately, the masses have proven themselves truly unworthy of that trust.

The real problem is that, with the spreading influence of the Internet, we are trading in authoritative and accurate for cheap and convenient. Wikipedia is only one example. Millions of people continue to flock to the Net for information on their health, their bank balances despite what we know about its certified fallibility according to security advisors and consultants across our globe. Studies by the American Medical Association and World Health Organization have found that the quality of medical information on the Web ranges from spotty to dismal. Whether you're after stock tips, or parenting advice, or movie reviews, it's all out there, free of charge, and generally worth exactly what you pay for it.

It'd be easy to just dismiss the Web, if not for the impact it has had on the so-called "old media." And the effects it is directly having on today's society. Terrified of being left behind in the rush online, newspapers and magazines simply dumped the contents of their publications onto the Internet for free. Meanwhile, aggregator sites like Google and Yahoo!News troll the Web and post headlines, photos and lead paragraphs from publications all around the world, eating into the audience for traditional newspapers and

collecting a share of the ad revenue. The sudden shift in the economics of newsgathering has exerted huge pressure on the traditional news gatherers, and major outlets from the New York Times to London's Daily Telegraph have responded by paring back their news staff. And so, in an era in which we're supposed to have universal access to more information from more varied sources around the world, there are fewer and fewer reporters on the ground digging up original information. And the companies in the business of providing credible, original reporting are finding it more and more difficult to survive.

In the place of hard information, the ‘World Wide Web' has ushered in the era of the amateur commentator. Rather than reporting the news, the Internet actually excels at allowing millions to analyze the news of the day on their blogs and message boards. "It is no exaggeration to conclude that the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country -- and indeed the world -- has yet seen," George Will, Newsweek's revered columnist, wrote a few years back. Sounds spectacular, but what's the great value of a participatory marketplace of mass speech if so few have anything to say that's worth buying?

Andrew Keen, a former Internet entrepreneur turned heretic, argues that this "digital utopianism" is playing havoc with our economy and politics. His forthcoming book, titled The Culture of the Amateur, is based on the idea that the onslaught of blogs, and social networking websites is primarily destroying our culture by celebrating mediocrity and devaluing talent. "The cult of the amateur is digital utopianism's most seductive delusion. . . It suggests, mistakenly, that everyone has something interesting to say," he wrote earlier this year, ironically, on his own blog.

Google News, Craigslist and the world army of bloggers have devalued journalism just as surely as Napster poisoned the market for recorded music. According to the PEW Internet and American Life Project, there are now more than 12 million bloggers in the United States alone, and more than a third of them consider what they do a form of journalism, even though little or no reporting is involved. There are certainly some interesting and insightful blogs, on a wide range of topics. But, in general, the more substantive the subject matter, the less reliable the commentary is. The vast majority of political blogs are deeply ideological and partisan, attract a core of like-minded contributors, and tend to devolve into vitriolic screeds or sophomoric insults. They feed on their contempt for the so-called mainstream media, which is derisively referred to as the "MSM," and is derided by both left and right as hopelessly biased and manipulative.

In a 2001 paper, Cass Sunstein, a professor at the University of Chicago Law School, described the "echo chamber" effect of blogs and message boards. Rather than fostering debate, moderation and common understanding, he argued, these sites have contributed to the polarization of our political culture. People gravitate toward sites that reflect their established point of view, and once comfortably ensconced in their political echo chamber, the participants take turns preaching to the assembled choir, reinforcing each other's ideas and biases, and denouncing anyone who might disagree.

Rather than promoting open discussion and greater understanding, the Net continues to feed the cynical perception that every form of traditional authority is based on lies and corruption. The much-hyped free market of ideas is a world in which the loudest and most outrageous assertion dominates the discussion. Everybody believes they are being oppressed by those opposed to them. The truth is what you already think it is, and no one can longer be trusted.

What would you want to know about, if you could know about anything? The Internet continues to pose this question daily, on a massive, global scale, and the answers we've provided are depressing.

Tim Berners-Lee, the man widely credited with inventing the World Wide Web, once said he envisioned an "an interactive sea of shared knowledge . . . immersing us as a warm, friendly environment made of the things we and our friends have seen, heard, believe or have figured out. I would like it to bring our friends and colleagues closer." But the public at large saw an open invitation to indulge vice on an unimaginable scale. A 1998 study by Forrester Research pegged the market for online porn at close to US$1 billion annually; a statistic that is growing exponentially. How much it has grown since then is the subject of bitter disagreement, but one company, Internet Filter Review, reported that between 1998 and 2003 the number of pornographic pages on the World Wide Web rose from 14 million to 260 million. The numbers are staggering.

But the burgeoning world of online gambling dwarfs porn for sheer earning power. In 2004, the American Gaming Association, a lobby group for the legalized U.S. casino industry, estimated that online gambling was a US$7-billion to $10-billion business and was growing at the rate of 20 per cent a year.

If porn bores you and you don't have the stomach for online poker, infidelity is also a booming business on the Web. A recent study by Jupiter Research found that 12 per cent of people registered with online dating services are married, and Ashley Madison, a Canadian-based site specifically aimed at married people looking to have an affair, now boasts more than 700,000 registered members. Morality and personal ethics is fast becoming an area that few are venturing as the truth of these statistics is becoming more transparent than we care to admit.

It's an oft-repeated exaggeration that the Internet is being used overwhelmingly for debauchery. It is far more accurate to say the vast majority of what we do online is utterly trivial. Last year, the top 10 Google searches were as follows: Janet Jackson, hurricane Katrina, tsunami, xBox 360, Brad Pitt, Michael Jackson, American Idol, Britney Spears, Angelina Jolie, and Harry Potter. Berners-Lee's interactive sea of shared knowledge is primarily concerned with two actors, three singers, a video game console, a TV show, a fictional character and two natural disasters.

Some might argue that the Internet bears no responsibility for our own moral frailties and frivolous interests. The fact that the Internet has shown us as we really are may be disappointing, but the failure is that of human nature. There are reasons, however, to

suspect that the Internet isn't just reflecting social values but is also helping to shape them. How many people do things online that they otherwise wouldn't because it's anonymous and consequence-free and behind closed monitors? Simply put -- the easier it gets to be bad, the worse we get.

Take, for example, the plague of academic plagiarism that has proliferated across university campuses over the past decade. In 2003, Rutgers University conducted the most comprehensive study to date on academic cheating, polling more than 18,000 students and 2,000 professors at 23 U.S. schools. An astonishing 38 per cent of undergraduates and 25 per cent of grad students admitted to using the Internet for some form of plagiarism in the past year, up from 10 per cent in a similar survey conducted two years earlier. About five per cent admitted to submitting an entire assignment cribbed from the Internet and passing it off as their own work, generally using one of the dozens of online "term-paper mills" that offer high-quality essays for sale on a staggering range of subjects. Perhaps most distressing, 44 per cent of the students said they see nothing wrong with cribbing material from the Internet.

Today's college students grew up with the World Wide Web, and many of them barely remember a world without it. Most wouldn't dare steal a DVD from a store shelf, but downloading the latest video release to watch with some friends is no big deal. Ask them if they consider it stealing, and they'll look at you like you're crazy. Why would buying a term paper or copying someone else's thesis be any different? They've come to expect that if it's available online, it's theirs to do with as they choose.

Alternatively, there are more insidious creatures in cyberspace than frat boys buying term papers. The Internet opened the floodgates to myriad forms of petty dishonesty, but real criminals looked upon its shroud of anonymity and saw an even greater opportunity. They made the Net a playground for their kind: hackers, spammers and con men. Stories of Trojan-horse programs stealing your passwords, worms burrowing into your hard drive, and spyware tracking your every move barely raise eyebrows anymore. We not only accept them, we expect them.

This year, Consumer Reports estimated that American consumers lost more than US$8 billion over the past two years to various online scams, and that approximately one in three Internet users will fall victim to some sort of cyber-crime in the course of a year, ranging from minor inconveniences, like small viruses affecting computer performance, to major frauds. Email fraud alone cost consumers US$630 million between 2004 and 2005.

David Wall is head of the School of Law at the University of Leeds in England, and recently finished a book called Cyber Crimes. He says that the world of crooks and con men has been forever changed by the evolution of the Internet. "The Internet has fundamentally changed crime, in that there is no longer any need to pull off a $1-million robbery, because it's now possible to do a million one-dollar robberies instead," he says. He points to spam as an example. Taken in isolation, each individual spam email is

nothing but a minor irritation. But taken as a whole it represents a massive, multi-million-dollar industry, much of it based on luring the gullible into fraudulent schemes.

Thanks to the Internet, it's no longer necessary for con men to spend time and effort identifying potential victims. Just blast out 100,000 emails and wait for the suckers to come to you. It doesn't matter if 99.9 per cent smell a rat. There's money to be made from exploiting the most gullible person in a thousand. Then, there is the darker side, Wall says. The Internet has also proven to be a very effective tool for grooming young individuals either for sexual purposes or for violent ones. We know, for example, that extremist groups around the world have turned to the Internet as a powerful recruiting tool. We know that detailed instructions on a wide range of illicit activities, from making crystal meth to building a bomb, are just a simple search away. And the sexual victimization of children online continues to happen at an alarming rate. Last month, the University of New Hampshire's Crimes Against Children Research Center released a poll that suggested 13 per cent of Web users between the ages of 10 and 17 had received unwanted sexual solicitations online at some point during the past year. Believe it or not, that was considered good news, as it was down from 19 per cent in 2000. But "aggressive solicitations," meaning situations in which a potential stalker had attempted to make contact with the child off-line, held steady at four per cent.

And yet, when it comes to protecting their kids, most parents have been slow to respond. According to the Alexandria, Va.-based Center for Missing and Exploited Children, only about a third of families use filtering or blocking software to monitor what their kids are doing online. A recent poll by Teenage Research Unlimited found 39 per cent of those polled said their parents know "very little" or "nothing" about what they do online.

Perhaps that's because we've become inured to the dangers of cyberspace in an incredibly short period of time, and once we grow accustomed to being violated, it erodes the sense that we, or anyone else, actually have a right to online security. If you lived in a neighbourhood where your child had a better than one-in-10 chance of being sexually propositioned on the street, and one out of every three people would be the victim of a crime in any given year, you'd almost certainly move if you could. But on the Internet, those odds are considered acceptable as long as we can continue to get instant updates on Brad Pitt and Angelina Jolie.

Clark Sampson, founder of Netspace, one of the earliest dot-coms, said the Internet would change everything and everyone, and it has. But change is not always progress. For everything, the Web has simplified, accelerated and proliferated; there is at least as much that it has destroyed, and we can't say we weren't warned.

The 1995 book Silicon Snake Oil, by renowned computer systems expert Clifford Stoll, now stands as one of the most distinct warnings about all we had to lose to the Internet. In summation, Stoll wrote that the rampant idealism that accompanied the Internet into the mainstream would end in disappointment. He recognized then what has since become obvious: what we thought of as a means of making connections is actually a deeply isolating and insular medium. Online community is an oxymoron along the lines of

virtual reality. "The computer hucksters have promoted a digital world which will not come to pass," Stoll said. As for the promise that simply by opening the lines of communication humanity would lay down arms and sing Kumbaya: "There are no simple technological solutions to social problems. There's plenty of distrust and animosity between people who communicate perfectly well. Access to a universe of information cannot solve our problems: we will forever struggle to understand one another."

And from now on, we will struggle within a wired world. The Internet has cost us trillions of dollars, and far more than that, but there's no going back. It is now so deeply entrenched and integrated into our personal culture -- in the way we speak and work and create and think -- that the only thing to do is to try to make it better, and hope that maybe we might somehow realize some of the dreams the idealists had when they invented the thing. Have we truly become more dehumanized and separated from the inherent truths that most of us were brought up on? Do we all finally need to take a long introspective look deep within our moral and ethical compass in a final effort to final put to rest the final question of who we really are and what or who is now the driving force of our existence? Is this a question we put to the philosophers and psychologists globally or more importantly to ourselves?

Terrorism and Internet Use

The great and many wondrous virtues of the Internet—its ease of access, lack of regulation, the potential audiences it caters to, and its fast flow of information, among others have been turned to the advantage of groups committed to terrorizing societies to achieve their selective goals. Today, most active terrorist groups have established their presence in some way or another on the Internet. Terrorism on the Internet is an extremely dynamic phenomenon: websites suddenly emerge, frequently modify their formats, and then swiftly disappear—or, in many cases, seem to disappear by changing their online address but retaining much the same content.

Terrorist websites target three different audiences: current and potential supporters; international public opinion; and enemy publics. The mass media, policymakers, and even security agencies have tended to focus on the exaggerated threat of cyber-terrorism and paid inadequate attention to the more routine uses made of the Internet. Those uses are numerous and, from the terrorists' perspective, invaluable. There are eight different ways in which contemporary terrorists are currently using the Internet, from psychological warfare and propaganda to highly instrumental uses such as fundraising, recruitment, data mining, and coordination of actions. While we must defend our societies against cyber-terrorism and Internet-savvy terrorists, we should consider the costs of applying counter-terrorism measures to the Internet. Such measures can hand authoritarian governments and agencies with little public accountability tools with which to violate privacy, circumvent the free flow of information, and restrict the freedom of expression, thus adding a heavy price in terms of diminished civil liberties to the high toll exacted by terrorism itself.

The story of the presence of terrorist groups in cyberspace has barely begun to be told. In 1998, around approximately half of the thirty organizations designated as "Foreign Terrorist Organizations" under the U.S. Antiterrorism and Effective Death Penalty Act of 1996 maintained websites; by 2000, virtually all terrorist groups had established their presence on the Internet. A scan of the Internet in 2004 revealed hundreds of websites served terrorists and their supporters. Intrestingly enough, when policymakers, journalists, and academics discuss the combination of terrorism and the Internet, they tend to focus on the overrated threat posed by cyber-terrorism or cyber-warfare (i.e., attacks on computer networks, including those on the Internet) and largely ignore the numerous uses that terrorists make of the Internet on a daily basis.

We turn the spotlight on these latter activities, identifying, analyzing, and illustrating ways in which terrorist organizations are exploiting the unique attributes of the Internet. We have witnessed a growing and increasingly sophisticated terrorist presence on the World Wide Web. Terrorism on the Internet, as has been discovered, is a very dynamic phenomenon: websites suddenly emerge, formats and layouts frequently modifed, and as swiftly and quietly as they appear they disappear. To locate terrorists' sites, numerous systematic scans of the Internet have revealed that feeding an enormous variety of names and terms into search engines, entering chat rooms and forums of supporters and sympathizers, and surveying the links on other organizations' websites to create and update our own lists of sites prove invaluable and beneficial.

The origins of the Internet, the characteristics of the new medium that make it so attractive to political extremists, the range of terrorist organizations active in cyberspace, and their target audiences is our primary focus. The heart of Internet terrorism is an analysis of eight different uses that terrorists continue to make use of on the Internet. These range from conducting psychological warfare to gathering information, from training to fundraising, from propagandizing to recruiting, and from networking to planning and coordinating terrorist acts. The Internet may be attractive to political extremists, but it also symbolizes and supports the freedom of thought and expression that helps distinguish democracies from their enemies.

Modern Terrorism and the Internet

The very decentralized network of communication that the U.S. security services created out of fear of the Soviet Union now serves the interests of the greatest enemy of the West's security services since the end of the Cold War: international terror. The roots of the modern Internet are to be found in the early 1970s, during the days of the Cold War, when the U.S. Department of Defence was concerned about reducing the vulnerability of its communication networks to nuclear attack. The Defense Department at that time decided to decentralize the entire system by creating an inter-connected web of computer networks. After twenty years of development and use by academic researchers and scholars, the Internet quickly evolved and expanded for commercial use in the late 1980s with a series of changed characteristics from its original state.

By 1994, the Internet connected more than 18,000 private, public, and national networks, with this number increasing daily. Hooked into those networks were about 3.2 million host computers and perhaps as many as 60 million users spread across the seven continents. The estimated number of users in the early years of the twenty-first century is over one billion—a surprising and simultaneously mind-blowing statistic in light of today's events.

As it emerged, the Internet was deemed as a triumphant exaltation and viewed as an integrator of cultures and a collective medium for businesses, consumers, and governments to communicate with one another. It appeared to offer insurmountable opportunities for the creation of a forum in which the "world" could meet and exchange ideas, stimulating and sustaining democracy throughout the world. However, with the enormous growth in the size and use of the network, utopian visions of the promises of the internet were challenged by the proliferation of pornographic and violent content on the "world wide web" and by the use of the Internet by extremist organizations of various kinds. Groups with very different political goals but united in their readiness to employ terrorist tactics started using the network to distribute their propaganda, communicate with their silent supporters, foster public awareness and even deploy their operations.

By its very essence, the internet has become an ideal arena for activity by several terrorist organizations. Most notably, terrorists groups taking advantage of the following characteristics provided by the Internet:

easy access;
little or no regulation, censorship, or forms of government control;
large audiences spread throughout the world;
anonymity of communication;
fast flow of information;
inexpensive development and maintenance of a web presence;
a multimedia environment (the ability to combine text, graphics, audio, and video and to allow users to download films, songs, books, posters, and so forth); and
the ability to shape coverage in the traditional mass media, which increasingly use the Internet as a source for stories.

Not a bad place to market and supply lethal information.

An Overview of Terrorist Websites

The benefits of the Internet have not gone unnoticed by terrorist organizations, regardless of their political orientation. Islamists fundamentalists, Marxists, nationalists, separatists, racists and anarchists: all find the Internet alluring. Today, almost all active terrorist organizations (which number more than 40) maintain websites, and many maintain multiple websites and use several different languages.

Content

Terrorist sites tend to provide a history of the organization, its activities, a detailed review of its social and political background and supporters, accounts of its notable exploits, detailed but not explicit biographies of its predominant leaders, founders, information on its political and ideological pursuits, fierce criticism of its enemies, and up-to-date news. Nationalist and separatist organizations generally display maps of the areas in dispute.

Audiences

An analysis of the content of the websites suggests three different audiences.

Current and potential supporters. Terrorist websites make enormous use of slogans and offer items for sale, including T-shirts, badges, flags, and multi-media material, all evidently aimed at sympathizers. Often, an organization will target its local supporters with a site in the local language and will provide detailed information about the activities and internal politics of the organization, its allies, and its competitors.

International public opinion. The international public, who are not directly involved in the conflict but who may have some interest in the issues involved, are courted with sites in languages other than the local tongue. Most sites offer versions in several languages.

Judging from the content of many of the sites, it appears that foreign journalists are also targeted. Press releases are often placed the websites in an effort to get the organization's point of view into the traditional media. The detailed background information is also very useful for international reporters.

Enemy publics

Efforts to reach enemy publics (i.e., citizens of the states against which the terrorists are fighting) are not as clearly apparent from the content of many sites. However, some sites do seem to make an effort to demoralize the enemy by threatening attacks and by encouraging feelings of guilt about the enemy's conduct and motives. In the process, they also seek to stimulate public debate in their enemies' states, to change public opinion, and to weaken public support for the governing regime.

Terrorists use of the Internet

We have identified eight different, and potentially overlapping, ways in which terrorists use the Internet. Some of these parallel the uses to which everyone puts the Internet—information gathering, for instance. Some resemble the uses made of the medium by traditional political organizations—for example, raising funds and disseminating propaganda. Others, however, are much more unusual and distinctive—for instance, hiding instructions, manuals, and directions in coded messages or encrypted files.

Psychological Warfare

Terrorism has often been conceptualized as a form of psychological warfare, and certainly many terrorists have sought to wage such a campaign throughout the Internet. They can use the Internet to spread disinformation, to deliver threats intended to distill fear and helplessness, and to disseminate horrific images of recent actions. Terrorists can also launch psychological attacks through cyber-terrorism, or, more accurately, through creating the fear of cyber-terrorism. "Cyber-fear" is generated when concern about what a computer attack could do (for example, bringing down an airline by disabling air traffic control systems, or disrupting national economies by wrecking the computerized systems that regulate economic and financial trends) is amplified until the public believes that an attack will occur. The Internet—an uncensored and powerful medium captures and carries stories, pictures, threats, or messages regardless of their validity or potential impact—is well suited to allowing even a small group to amplify its message and exaggerate its importance and the threat it can pose.

Al Qaeda combines multimedia propaganda and advanced communication technologies to create a very sophisticated form of psychological warfare. Osama bin Laden and his numerous followers concentrate their propaganda efforts on the Internet, where visitors to al Qaeda's numerous websites and to the sites of sympathetic, above-ground organizations can access pre-recorded videotapes and audiotapes, CD-ROMs, DVDs, photographs, and announcements. Despite the massive onslaught it has sustained in recent years—the arrests and deaths of many of its members, the dismantling of its operational bases and training camps in Afghanistan, and the smashing of its bases in the Far East—al Qaeda has been able to conduct an impressive terror campaign. Since the events of September 11, 2001, the organization has embedded its websites with a string of announcements of an impending "large attack" on potential U.S. targets. These warnings have received considerable media coverage, which has assisted to generate a widespread sense of fear and insecurity amongst audiences throughout the world, especially within the United States.

Interestingly, al Qaeda has consistently proclaimed on its websites that the destruction of the World Trade Center has inflicted psychological damage, as well as concrete damage, on the U.S. economy. The attacks on the Twin Towers are depicted as an assault on the trademark of the U.S. economy, and therefore provided remarkable evidence of their effectiveness is seen in the weakening of the dollar, the decline of the U.S. stock market after 9/11, and a supposed loss of confidence in the U. S. economy both within the United States and elsewhere. Parallels are drawn between the decline and ultimate demise of the Soviet Union. One of bin Laden's recent publications, posted on the web, declared that "America is in retreat by the Grace of Almighty and economic attrition is continuing up to today. But it needs further blows. The young men need to seek out the nodes of the American economy and strike the enemy's nodes."

Publicity and Propaganda

The Internet has significantly expanded the opportunities for terrorists to secure their public rebellion. Until the global emergence of the Internet, terrorists' hopes of winning

publicity for their causes and activities depended on attracting the attention of television, radio, or print media. These traditional channels have "selection thresholds" (multistage processes of editorial selection) that terrorists often cannot reach. No such thresholds exist on the terrorists' own websites. The fact that many terrorists have direct control over the content of their message offers tremendous opportunities to shape how they are perceived by different target audiences and to manipulate their own image and the image of their enemies.

Most terrorist sites do not celebrate their violent activities. Instead, regardless of the terrorists' agendas, motives, and location, most sites emphasize two issues: the restrictions placed on freedom of expression and the plight of comrades who are now political prisoners. These resounding issues resonate powerfully with their own supporters and are also calculated to elicit sympathy from Western audiences that cherish freedom of expression and frown upon measures to silence any political opposition. Enemy publics, too, may be targets for these complaints insofar as the terrorists, by emphasizing the antidemocratic nature of the steps taken against them, try to create feelings of unease and shame among their enemies. The terrorists' protest at being muzzled, it may be noted, is particularly well suited to the Internet, which for many users is the symbol of a free, unfettered, and uncensored conduit of communication.

Terrorist sites commonly employ three rhetorical structures, all justify their continuous reliance on violence and fear. The first one is the claim that the terrorists have no choice other than to turn to violence. Violence is presented as a necessity forced upon the weak as the only means with which to respond to an oppressive enemy. While the sites avoids mentioning how the terrorists continue to victimize others, the forceful actions of the governments and regimes that combat the terrorists are heavily emphasized and characterized with terms such as "slaughter," "murder," and "genocide." The terrorist organization is depicted as constantly persecuted, its leaders subject to assassination attempts and its supporters massacred, its freedom of expression curtailed, and its adherents arrested. This tactic, which portrays the organization as small, weak, and hunted down by a strong power or a strong state, turns the terrorists into the underdog.

A second rhetorical structure related to the legitimacy of the use of violence is the demonizing and delegitimization of the enemy. The members of the movement or organization are presented as freedom fighters, forced against their will to use violence because a ruthless enemy is crushing the rights and freedom of their people or group. The enemy of the movement or the organization is the real terrorist, many sites insist: "Our violence is tiny in comparison to his aggression" is a common argument. Terrorist rhetoric tries to shift the responsibility for violence from the terrorist to the adversary, which is accused of displaying its brutality, inhumanity, and immorality.

The third rhetorical device is to make extensive use of the language of nonviolence in an attempt to counter the terrorists' violent image. Although these are violent organizations, many of their sites claim that they seek peaceful solutions, that their ultimate aim is a diplomatic settlement achieved through negotiation, compromise, and international pressure on a repressive government.

Data Mining

The Internet can be viewed as a vast digital library. The World Wide Web alone offers about a billion pages of information, most of it free—and much of it, of interest to terrorist organizations. Terrorists, for instance, can learn from the Internet a wide variety of details about targets such as transportation facilities, nuclear power plants, public buildings, airports, and ports, and even about counter-terrorism measures. They use the Internet to collect intelligence on targets, especially critical economic nodes, and modern software enables them to study structural weaknesses in facilities as well as predict the cascading failure effect of attacking certain systems." According to former Secretary of Defense Donald Rumsfeld, speaking on January 15, 2003, about an al Qaeda training manual recovered in Afghanistan which tells its readers, "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy."

Like many other Internet users, terrorists have access not only to maps and diagrams of potential targets but also to imaging data on those same facilities and networks that may reveal counterterrorist activities at a target site. One confiscated al Qaeda computer contained engineering and structural features of a dam, which had been downloaded from the Internet and which would enable al Qaeda engineers and planners to simulate catastrophic failures. Other confiscated computers provided U.S. investigators with evidence that al Qaeda operators spent time on websites that offer software and programming instructions for the digital switches that run power, water, transportation, and communications grids. Numerous tools are available to facilitate such data collection, including search engines, e-mail distribution lists, and chat rooms and discussion groups. Many websites offer their own search tools for extracting information from databases on their sites. Word searches of online newspapers and journals can likewise generate information for use by terrorists; some of this information may be available in the traditional media, but online searching capabilities allow terrorists to capture it anonymously and with very little effort or expense.

Fundraising

Like many other political organizations, terrorist groups use the Internet to raise funds. Al Qaeda, for instance, has always depended heavily on donations, and its global fund-raising network is built upon a foundation of charities, non-profit organizations, and other financial institutions that use websites and Internet-based chat rooms and forums. The Sunni extremist group Hizb al-Tahrir uses an integrated web of Internet sites, stretching from Europe to Africa, which asks supporters to assist the effort by giving money and encouraging others to donate to the cause of jihad. Banking information, including the numbers of accounts into which donations can be deposited, is provided on a site based in Germany. The fighters in the Russian breakaway republic of Chechnya have likewise used the Internet to publicize the numbers of bank accounts to which sympathizers can contribute. (One of these Chechen bank accounts is located in Sacramento, California.) The IRA's website contains a page on which visitors can make credit card donations.

Internet demographics allow terrorists to identify users with sympathy for a particular cause or issue. These individuals are then asked to make donations, typically through e-mails sent by a front group (i.e., an organization broadly supportive of the terrorists' aims but operating publicly and legally and usually having no direct ties to the terrorist organization). For instance, money benefiting Hamas has been collected via the website of a Texas-based charity, the Holy Land Foundation for Relief and Development (HLF). The U.S. government seized the assets of HLF in December 2001 because of its ties to Hamas. The U.S. government has also frozen the assets of three seemingly legitimate charities that use the Internet to raise money—the Benevolence International Foundation, the Global Relief Foundation, and the Al-Haramain Foundation—because of evidence that those charities have funneled money to al Qaeda.

The Internet can be used not only to solicit donations from sympathizers but also to recruit and mobilize supporters to play a more active role in support of terrorist activities or causes. In addition to seeking converts by using the full panoply of website technologies (audio, digital video, etc.) to enhance the presentation of their message, terrorist organizations capture information about the users who browse their websites. Users who seem most interested in the organization's cause or well suited to carrying out its work are then contacted. Recruiters may also use more interactive Internet technology to roam online chat rooms and cyber-cafes, looking for receptive members of the public, particularly young people. Electronic bulletin boards and user nets can also serve as vehicles for reaching out to potential recruits.

Networking

Many terrorist groups, among them Hamas and al Qaeda, have undergone a transformation from strictly hierarchical organizations with designated leaders to affiliations of semi-independent cells that have no single commanding hierarchy. Through the use of the Internet, these loosely interconnected groups are able to maintain contact with one another—and with members of other terrorist groups. In the future, terrorists are increasingly likely to be organized in a more decentralized manner, with arrays of various groups linked by the Internet and communicating and coordinating horizontally rather than vertically.

Several reasons explain why modern communication technologies, especially computer-mediated communications, are so useful for terrorists in establishing and maintaining networks. First, new technologies have greatly reduced transmission time, enabling dispersed organizational actors to communicate swiftly and to coordinate effectively. Second, new technologies have significantly reduced the cost of communication. Third, by integrating computing with communications, they have substantially increased the variety and complexity of the information that can be shared.

The Internet connects not only members of the same terrorist organizations but also members of different groups. For instance, dozens of sites exist that express support for terrorism conducted in the name of jihad. These sites and related forums permit terrorists

in places such as Chechnya, Palestine, Indonesia, Afghanistan, Turkey, Iraq, Malaysia, the Philippines, and Lebanon to exchange not only ideas and suggestions but also practical information about how to build bombs, establish terror cells, and carry out attacks.

Sharing Information

The World Wide Web is home to dozens of sites that provide information on how to build chemical and explosive weapons. A much larger manual, nicknamed "The Encyclopedia of Jihad" and prepared by al Qaeda, runs tousands of pages long and is distributed through the Internet. This manual offers detailed instructions on how to establish an underground organization and execute attacks. One al Qaeda laptop found in Afghanistan had been used to make multiple visits to a French site run by the Société Anonyme (a self-described "fluctuating group of artists and theoreticians who work specifically on the relations between critical thinking and artistic practices"), which offers a two-volume Sabotage Handbook with sections on topics such as planning an assassination and anti-surveillance methods.

Planning and Coordination

Terrorists use the Internet not only to learn how to build bombs but also to plan and coordinate specific attacks. Al Qaeda operatives relied heavily on the Internet in planning and coordinating the attacks of September 11. Thousands of encrypted messages that had been posted in a password-protected area of a website were found by federal officials on the computer of arrested al Qaeda terrorist Abu Zubaydah, who reportedly masterminded the September 11 attacks. The first messages found on Zubaydah's computer were dated May 2001 and the last were sent on September 9, 2001. The frequency of the messages was highest in August 2001. To preserve their anonymity, the al Qaeda terrorists used the Internet in public places and sent messages via public e-mail. Some of the September 11 hijackers communicated using free web-based e-mail accounts.

Hamas activists in the Middle East, for example, use chat rooms to plan operations and operatives exchange e-mail to coordinate actions across Gaza, the West Bank, Lebanon, and Israel. Instructions in the form of maps, photographs, directions, and technical details of how to use explosives are often disguised by means of steganography, which involves hiding messages inside graphic files. Sometimes, however, instructions are delivered concealed in only the simplest of codes. Mohammed Atta's final message to the other eighteen terrorists who carried out the attacks of 9/11 is reported to have read: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." (The reference to the various faculties was apparently the code for the buildings targeted in the attacks.)

Conclusion

In a briefing given in late September 2001, Ronald Dick, assistant director of the FBI and head of the United States National Infrastructure Protection Center (NIPC), told reporters that the hijackers of 9/11 had used the Internet, and "used it well." Since 9/11, terrorists have only sharpened their Internet skills and increased their web presence. Today, terrorists of very different ideological persuasions—Islamist, Marxist, nationalist, separatist, and racist—have learned many of the same lessons about how to make the most of the Internet. The great virtues of the Internet—ease of access, lack of regulation, vast potential audiences, fast flow of information, and so forth—have been turned to the advantage of groups committed to terrorizing societies to achieve their goals.

First, we must become better informed about the uses to which terrorists put the Internet and be better able to monitor their activities. As noted at the outset of this report, journalists, scholars, policymakers, and even security agencies have tended to focus on the exaggerated threat of cyber-terrorism and paid insufficient attention to the more routine uses made of the Internet. Those uses are large in number and, from the terrorists' perspective, invaluable. Hence, it is imperative that security agencies continue to improve their ability to study and monitor terrorist activities on the Internet and explore measures to limit the usability of this medium by modern terrorists.

Second, while we must better defend our societies against terrorism, we must not in the process erode the very qualities and values that make our societies worth defending. The Internet is in many ways an almost perfect embodiment of the democratic ideals of free speech and open communication; it is a marketplace of ideas unlike any that has existed before. Unfortunately, the freedom offered by the Internet is vulnerable to abuse from groups that, paradoxically, are themselves often hostile to uncensored thought and expression. But if, fearful of further terrorist attacks, we circumscribe our own freedom to use the Internet, then we hand the terrorists a victory and deal democracy a blow. We must not forget that the fear that terrorism inflicts has in the past been manipulated by politicians to pass legislation that undermines individual rights and liberties. The use of advanced techniques to monitor, search, track, and analyze communications carries inherent dangers. Although such technologies might prove very helpful in the fight against cyber terrorism and Internet-savvy terrorists, they would also hand participating governments, especially authoritarian governments and agencies with little public accountability, tools with which to violate civil liberties domestically and abroad. It is easily recognized that the long-term implications could be profound and damaging for democracies and their values, adding a heavy price in terms of diminished civil liberties to the high toll exacted by terrorism itself.

Final Thoughts

Terrorists fight their wars in cyberspace as well as on the ground. However, while politicians and the media have debated the dangers that cyber-terrorism pose to the Internet, surprisingly little is known about the threat posed by terrorists' use of the Internet. Today, terrorist organizations and their supporters maintain hundreds of websites, exploiting the unregulated, anonymous, and easily accessible nature of the Internet to target an array of messages to a variety of audiences. This not only analyzes

how the Internet can facilitate terrorist operations but also illustrates the point that many specific details can be derived exclusively from the information publically advertised via extensive exploration of the World Wide Web.

Warnings of internet overload

As the flood of data across the internet continues to increase, there are those that say sometime soon it is going to collapse under its own weight. But that is what they said last year.
Web traffic in the 90s was much smaller than today

Back in the early 90s, those of us that were online were just sending text e-mails of a few bytes each, traffic across the main US data lines was estimated at a few terabytes a month, steadily doubling every year.

But the mid 90s saw the arrival of picture-rich websites, and the invention of the MP3. Suddenly each net user wanted megabytes of pictures and music, and the monthly traffic figure exploded.

For the next few years we saw more steady growth with traffic again roughly doubling every year.

But since 2003, we have seen another change in the way we use the net. The YouTube generations wants to stream video, and download gigabytes of data in one go.

"In one day, YouTube sends data equivalent to 75 billion e-mails; so it's clearly very different," said Phil Smith, head of technology and corporate marketing at Cisco Systems.

"The network is growing up, is starting to get more capacity than it ever had, but it is a challenge.

"Video is real-time, it needs to not have mistakes or errors. E-mail can be a little slow. You wouldn't notice if it was 11 seconds rather than 10, but you would notice that on a video."
Spending our inheritance

Perhaps unsurprisingly, every year someone says the internet is going to collapse under the weight of the traffic.

The net's backbone was built thanks to the 90s dotcom boom

Looking at the figures, that seems a reasonable prediction.

"Back in the days of the dotcom boom in the late 90s, billions of dollars were invested around the world in laying cables," said net expert Bill Thompson.

"Then there was the crash of 2000 and since then we've been spending that inheritance, using that capacity, growing services to fill the space that was left over by all those companies that went out of business."

Router reliability

Much more high-speed optic fibre has been laid than we currently need, and scientists are confident that each strand can be pushed to carry almost limitless amounts of data in the form of light.

But long before a backbone wire itself gets overloaded, the strain may begin to show on the devices at either end - the routers.

"If we take a backbone link across the Atlantic, there're billions of bits of data arriving every second and it's all got to go to different destinations," explained Mr. Thompson.

The real issue that people are going to face, and are already noticing at home, is that ISPs are starting to cut back on the bandwidth that is available to people in their homes Bill Thompson, net expert "The router sits at the end of that very high speed link and decides where each small piece of data has to go. That's not a difficult computational task, but it has to make millions of decisions a second."

The manufacturer of most of the world's routers is Cisco. When I pushed them on the subject of router overload, they were understandably confident.

"Routers have come a long way since they started," said Mr. Smith. "The routers we're talking about now can handle 92 terabits per second.

"We have enough capacity to do that and drive a billion phone calls from those same people who are playing a video game at the same time they're having a text chat."

Congestion

Even if the routers can continue to take what the fibre delivers, there is another problem - the internet is not all fibre.

A lot of the end connections, the ones that go to our individual home computers, are made of decades-old copper.

"The real issue that people are going to face, and are already noticing at home, is that ISPs are starting to cut back on the bandwidth that is available to people in their homes," said Mr. Thompson. "They call it bandwidth shaping.

"They do this because they have a limited capacity to deliver to 100 or 200 homes, and if everybody's using the internet at the same time then the whole thing starts to get congested. Before that happens they cut back on the heavy users."
Obstacles

But digital meltdown is not the only threat facing the net. There are other, more sudden, real world hazards, which the net has to protect against.

Anything from terror attacks to, would you believe it shark bites, can and have taken out major links and routers.

It only takes an earthquake, as we saw at the end of last year, to take out a significant segment of internet infrastructure

Paul Wood, MessageLabs "There's a perception that the internet is very resilient," said Paul Wood, senior analyst of security firm MessageLabs. "The way it was designed means that if any particular part of it is disrupted then the traffic will find another route.

"It only takes an earthquake, as we saw at the end of last year, to take out a significant segment of internet infrastructure. Then the traffic finds another route, but it goes over a very slow route, which then becomes saturated and can't handle the bandwidth. Then you lose the traffic and that part of the world goes dark for a while."

For decades the internet has kept pace with our demands on it. And demand continues to grow.

And the service providers will continue to insist that the net will survive, and the doomsayers will continue to insist that it is just about to collapse.

Banking, Cyber Crime, Hacking
A New Look at Internet Security

Internet security is big news today and is growing at an exponential rate. According to the latest National Opinion Poll, as of January 2007, almost half of UK citizens still harbour a "deep mistrust" of the Internet due to security concerns. This does not include statistics from North America so I am sure the overall global numbers will indeed be quite alarming once available. The premise of ideas however is consistent.

The House of Lords Select Committee on Science and Technology, meanwhile, is currently orchestrating a major enquiry into personal Internet security. Their Lordships observed wisely that "With the ever growing use of home computers, the spread of broadband, and the rise in internet banking and commerce the importance of proper internet security measures has never been greater."

How well equipped is our Government to combat the threat of cyber crime that currently exists?

Response to the consultation has been extensive, and the Lords Select Committee has been hearing evidence since consultation closed in October 2006, from parties as varied as the Internet Service Providers Association, Richard Clayton of the Cambridge Security Lab, John Carr of the Children's Charities' Coalition on Internet Safety, Jonathan Zittrain of the Oxford Internet Institute and many speakers from commercial bodies such as eBay, as well as the ICO, OFT and DTI.

Meanwhile the councils have been more concerned with the public aspects of cyber security. In the last few years we have seen a rash of communications from them on topics such as information system security, critical infrastructure protection and denial of service attacks. ENISA, the European information Security Agency established in 2004, is becoming increasingly active. Despite all this, most businesses and citizens in Europe did still not take the threat posed by cyber-insecurity seriously.

Unsurprisingly, a program followed this damning summary quickly and a Draft Directive on Critical Infrastructure Protection announced at the end of 2006.

The security and economy of the European Union as well as the well being of its citizens depends on certain infrastructure and the services they provide. The destruction or disruption of infrastructure providing key services could entail the loss of lives, the loss of property, a collapse of public confidence globally.

At root here, of course, is the fear not of simple hacking by domestic criminals or bored teens, nor even of blackmail by gangs of Estonian extortionists, but, in the post 9/11 world, of serious terrorist activity directed at nuclear plants, hospitals, automated transport, air traffic control, banking systems and domain name servers: the catalogue of possible targets is endless. Accordingly, the Draft Directive proposes the designation of a European Critical Infrastructure which will receive special protection and attention.

The Appendix blandly designates "The Internet" in its entirety as part of this ECI. When and if the Directive passes, it will be fascinating to see how the fairly onerous responsibilities of the Directive – e.g. the creation and implementation of an Operator Security Plan - can be applied to every part of the Internet, including small one man ISPs and universities, etc. – but that is a problem for later discussion.

For now, the point of this article is that, in the realm of Internet security, the personal is also the public (an adaptation of the old feminist adage that the personal is political?) and that the two cannot, and should not, be separated if we are to attain the nirvana of a safe and secure critical infrastructure and Internet. Nor can consideration of personal security and privacy threats to consumers; usefully be separated from the home security practices of those same individuals. In previous work on spam and denial of service, it was observed that most mal-doing on the Internet is now orchestrated via unknowing networks of thousands if not millions of "zombie" or "bot" computers. Such computers

are typically home consumer machines, attached to "always on" broadband facilities, which have been infected by viruses or other types of software so that unknown to their legitimate owner, and usually without degradation of their ordinary capabilities, they perform the bidding of a "zombie master". Hacking, denial of service, virus dissemination, theft of personal data, spamming, key-logging, click fraud, ID fraud and other cyber exploits are all now almost wholly orchestrated via such zombie networks.

Why we ask? A number of reasons. For exploits such as denial of service, superior firepower is needed to knock down the servers of a bank or a major corporation – hence DoS becomes distributed denial of service. The activity of zombies is almost untraceable back to the actual criminal masterminds, the zombie masters (or their paymasters). Criminal activity can be handled remotely by botnets while the zombie masters stay safely at home in safe havens like parts of the Former Soviet Union. And making or acquiring zombies is child's play nowadays: botnets can be bought for remarkably low prices, and zombie-making virus kits are readily available on the net. Technical knowledge is thus no longer necessary, and zombie networks are simply becoming another tool of the international criminal and gangster (and terrorist?) fraternity.

What are we to do about this? Grand plans to safeguard critical Infrastructure are clearly important, but they are, to some extent, a case of safeguarding the stable after the horses have become zombies. Would it not be better to plan to make a more secure Internet from now on, as well as to put resources into fortifying our airports and power plants from attacks from the insecure Internet we have currently created? Criminal law is also a rather blunt and expensive tool with which to attack this threat. Criminal cross-border investigations may catch a few zombie masters and international hackers, but the resources needed are vast and the rewards few. Arguably, updating and enforcing cyber-criminal law is something of a red herring; an administrative, regulatory or technical solution might work better to produce a safer Net first, and then we can worry about catching and punishing the actual wrongdoers, safe behind territorial and technical anonymity, later.

In previous work and statements made by well-respected journalists, it was argued "security was for everyone, not just for Christmas". What does this mean? Catching and prosecuting zombie masters is the hardest and least useful part of the puzzle to solve.

Instead, we can more helpfully look elsewhere for aid. For a start, we could ask the software writers to write better software, with fewer vulnerabilities, and therefore less need for frequent patching and updating to plug exploitable holes. (A tall order, says the software industry, but one that needs tackling sooner rather than later.) We could ask industry and the public sector to make sure their machines run up to date, patched software, and perhaps that they show a preference for open source software which is often more secure and less prone to attack than some ubiquitous proprietary software.

We could ask ISPs to scan the data traffic going to and from computers attached to their networks for unusual patterns of traffic, and then to cut those likely zombies off from the Internet until they can be properly dismissed. We could even ask then to take on remote

patching and updating of the operating systems and software on consumer machines, though this has multiple problems, of cost, liability, autonomy and consumer choice. It would however get round the problem of consumer ignorance and inertia as to computer security. We could alternately try to educate consumers in "safe software": to use virus checkers, adware and spyware blockers, and firewalls conscientiously.

But will we succeed? People do not want to fiddle with their PCs and Macs, to take the back off, or to get under the hood. They do not have the knowledge, the skills or, usually the incentive (zombified machines work fine, the threat posed is to others) and in some cases, they are actively scared of getting their "hands dirty".

Until the computer-savvy twenty-something generation rules the world, we may have to think again about an interim solution to cope with domestic machines, zombies and computer insecurity.

Let us think about cars. When automobiles arrived on the scene, they were clearly inherently dangerous objects. They went too fast, were driven badly by ignorant, uneducated owners and scared the horses. Naturally a man was instructed to walk in front of them with a red flag and they were restricted to an anecdotal 5 mph.

Today cars go far, far faster (but are, admittedly, a lot safer) but are still inherently dangerous objects. They are driven by people who, just as in the 19th century, largely do not understand how their car works, and have no idea how to maintain it in a state of safety. How do we as a society manage the risks of dangerous cars and consumer ignorance?

Well, in several ways. There is of course the criminal law; we know we are not allowed to drink and drive, or to drive dangerously without possibility of penalty. But this is not really the main way in which "car insecurity" is controlled. There are instead a number of regulatory and administrative means, far more effective than criminal law, which keeps our roads, to a reasonably large extent, safe. You cannot, for a start, drive a car without a license. That implies a certain degree of education and knowledge of the rules of the road. You cannot drive without insurance. That means that if you do cause damage to someone else due to your insecurity they are at least always compensated. Both the license and the insurance systems are enforced, cleverly, not (in the main) by resource intensive police checks, but by the requirement that both be displayed to obtain a tax disc: and the tax disc system combined with a national car registration database allows for effective checking of who is properly "secured" by an automated computer system. Policing such a system then becomes relatively trivial.

Can we learn from this for computer insecurity, with reference to consumers and zombies? It is clearly impossible, practically, politically and ethically, to require every consumer – including the ignorant, the poor and even the elite – to be legally responsible for keeping their computer in a state of reasonable security. We can try and educate them but we probably cannot impose a "computer-driving license". But perhaps we can allow them to offload that responsibility, as we do with cars. Cars are safe in part because after

a certain age they have to be checked over by a responsible garage and certified as fit for the road. Without such an "MOT", again, a tax disc cannot be obtained. Again, we cannot probably reasonably demand that home owners have their computers checked over as safe by a travelling "computer MOT man" – the issues of invasion of privacy, surveillance and inertia are too great, and, anyway, one day after the MOT man had been round the computer would be hit by a new virus. But we could present a number of alternatives.

Suppose a basic obligation is placed on every networked computer owner to keep that computer reasonably secure. This obligation could be met by:
Self-vigilance

This is fine for the commercial and public sector where resources such as IT departments exist to keep computers safe. It is also fine for home computer owners who feel capable of keeping their own machines secure ("geeks" as they are known in the trade). Alternately, for the vast majority of individuals (and small businesses?) who do not have computer skills, another option would be:
Subscribing to an ISP who undertakes security measures for you

Such services are already beginning to be available on the market at reasonable rates. Some ISP's offer a range of industry level secure ISP services to consumers. A legal obligation of security on consumers, which could be met by signing up to, an accredited secure ISP service would quickly inspire a competitive market of "safe ISPs". Exactly what the ISP would have to offer would have to be worked out and supervised – patching, updating, scanning, closing of ports, remote operation of virus checkers and firewalls? Model "safe ISP" contracts could perhaps be drafted, drawn up in collaboration between the ISP and the DTI, and then kite marked. The strength of this suggestion is that ISPs are being asked to provide a business service at market rates; not to take on a role as guardians of the Internet for free, which there is no reasonable case for imposing on them.

Insurance

In this system, every consumer should also be asked to take on cyber security insurance. Currently this is a very fledgling market, but a legal obligation would immediately create a competitive market. If an individual breached their obligation of reasonable security – e.g. by choosing option 1 of self vigilance and failing to keep their computer adequately patched – then at least insurance would be available to pay towards damage caused to third parties. This should also provide an incentive not to choose option 1 out of inertia, as the result of calling on cyber-insurance would be that the cost of the next premium should rise considerably. (Problems might arise with causality and share of blame – if a network of 10,000 bots attacks IBM, what is the responsibility of one zombie? -but these could be overcome if insurance pay-outs were made into a general pot out of which compensation was paid to victims. Clearly, there is a lot of detail to be filled in here.)

This is just one back of an envelope scheme, which seeks to use (primarily) administrative rather than criminal law to regulate cyber-insecurity; there could be others. But the underlying message is to ask both the Select Committee and the security councils worldwide to think about ways of securing home user computers as well as critical infrastructure; to try to create a safer Internet and not just try to deal with the consequences of an unsafe one. To reshape and coin an old aphorism, in this domain, security really does begin at home.


Malware
Hackers
Viruses
Worms
Malware
Adware
Spyware
Spam
Spam
Phishing
Rootkits
Viruses
Malware
Hackers
Worms
Trojans