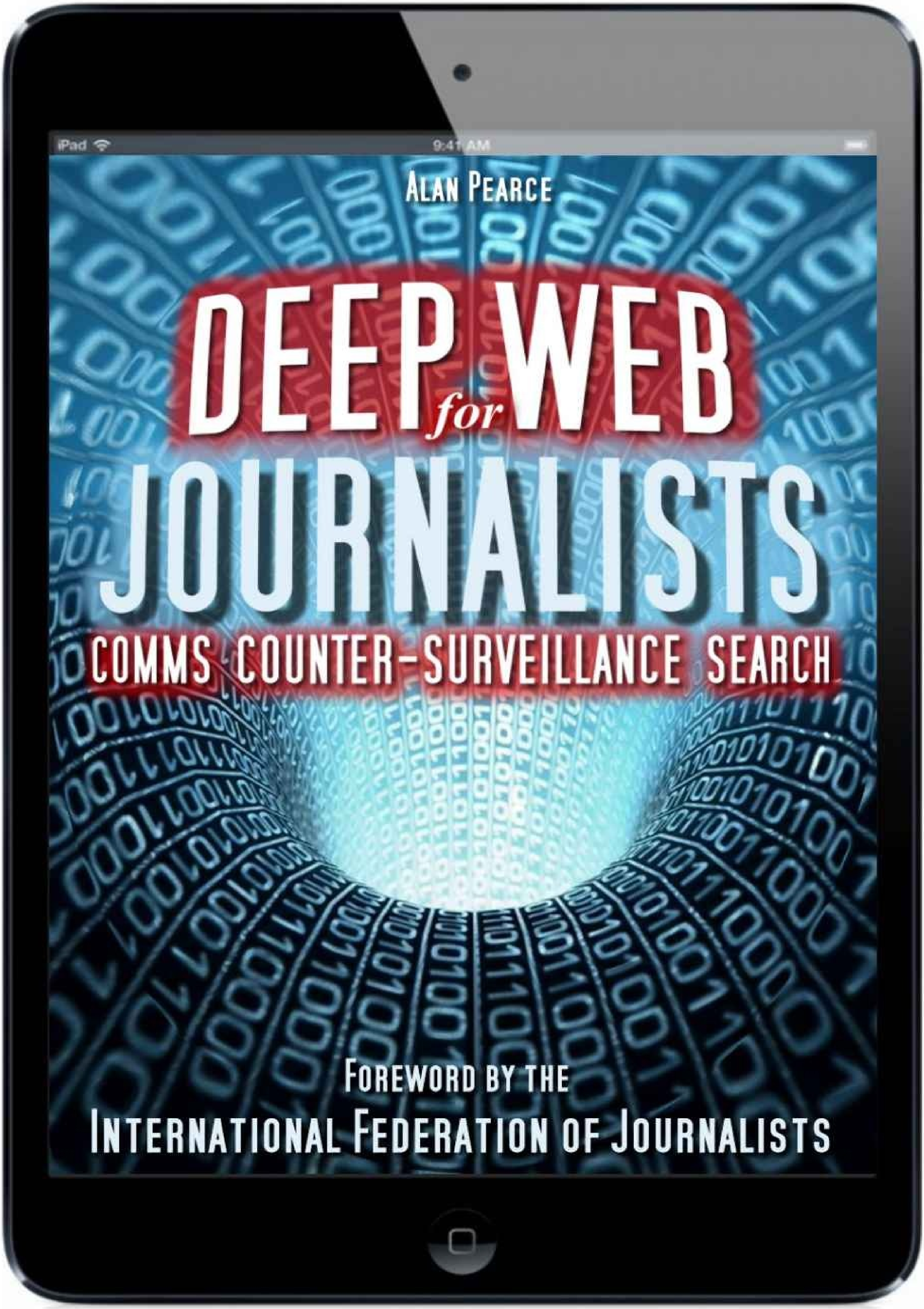

Alan Pearce

Deep Web for Journalists

Comms Counter-Surveillance Search

Foreword by the International Federation of Journalists

Deep Web for Journalists:
Comms, Counter-surveillance, Search

*****

By Alan Pearce
Edited by Sarah Horner
*

ASIN: B00CSW1KUW
v 0:4

www.deepwebguides.com

Table of Contents

Foreword by the International Federation of Journalists

Navigating the Dangerous Cyber Jungle

Online media safety is of the highest importance to the International Federation of Journalists. After all, the victims are often our members.

The IFJ is the world's largest organization of journalists and our focus is on ways and means to stop physical attacks, harassment and the killing of journalists and media staff. In an age where journalism – like everything else in modern life – is dominated by the Internet, online safety is emerging as a new front.

In this new war, repressive regimes now keep a prying eye on what journalists say, write and film. They want to monitor contacts and they want to suppress information. For journalists, this has become a dangerous game of cat and mouse.

Journalists are on notice – "everything you say and write will be taken down and used to track you and your contacts down."

This merciless pursuit for control of online communications has considerably raised the stakes in the current safety crisis facing journalists and the media. We are living at a time of unprecedented levels of violence against the Press.

Now we need to master the skills necessary to navigate this dangerous cyber jungle.

'Deep for Web Journalists' is the tool to achieve that. This engaging book by Alan Pearce charts a path to online knowledge which should be compelling reading for all journalists.

It offers an uncompromising diagnosis of the perils of online communications and should shatter the confidence many of us place in the unguarded ways of working online. This book offers simple advice to cover our tracks online and ensure that journalists are not an easy target for online press freedom predators.

Read all about 'Deep for Web Journalists'!

Jim Boumelha,

President, International Federation of Journalists

Introduction

Journalism has been transformed by the Internet and the Internet has opened journalists to levels of surveillance that would have horrified George Orwell.

Being a journalist in 2013 is more dangerous than it ever was. In addition to the usual threats, beatings, murders and war casualties, we are now being actively targeted online by intelligence agencies, law enforcement and others.

These days it is not just journalists working in repressive regimes that need worry. We now know that the US and its cyber-allies – Britain, Canada, Australia and New Zealand – actively monitor domestic journalists in their mass surveillance of the Internet.

Edward Snowden has warned journalists that they are special targets and he has expressed surprise that news organizations rarely have any counter-measures in place.

They harvest our contacts and monitor our telephone logs. They read our emails and texts. They follow our every move online and they keep tabs on every line we write.

Washington monitors domestic journalists under the National Operations Center’s Media Monitoring Initiative and other US agencies are now targeting foreign journalists following recent amendments to the Foreign Intelligence Surveillance Act. Information is regularly shared with foreign agencies and the private sector.

Any US-owned “remote computing service” – meaning any public computer storage or processing service – is open to scrutiny by US intelligence agencies without the need for a warrant.

Start researching sensitive subjects or visiting extremist websites and a tracking device will quickly be planted in your computer to follow you around and report back. It is all too easy for an algorithm to misconstrue your browsing activities and for alarm bells to be set off.

Mobile devices are not secure unless you make them so. If somebody wants to know where you are at this precise moment, your smartphone will tell them – even if it is turned off.

Not every journalist needs be concerned about this. But it is important to know how to operate securely should you ever need to. If you can’t offer confidentiality, you are compromised.

So how can we safeguard our sources and communicate without being overheard? How can we conduct sensitive research without having to watch our backs?

In Britain, where journalists are being arrested faster than they are in Russia, the police demand access to *all* their stored data. If they don’t hand over passwords to encrypted files they face a lengthy jail term.

This book will show how to overcome these threats without any real technical skills. Using freely downloadable programs and apps, you can block intruders, mask your identity online, set up secure communications, and transfer and store any amount of data without anyone being any the wiser.

But to do this we need to employ the black arts. When governments say they must have access to all our computer data to thwart terrorists, pedophiles, money-launderers and drug barons, they are not telling the whole truth. Only the most hapless terrorist is going to give anything away in an email. The seriously bad guys, as a rule, use the Deep Web.

Alan Pearce

June 2013

What is the Deep Web and why is it useful to Journalists?

Simply put, the Deep Web encompasses everything that the conventional search engines can't find. Google may index around 15 billion pages but it only seeks out those that want to be found or have conventional addresses that end in *.com* or *.org*, etc. It skims the surface and offers up the most popular results.

Largely unnoticed by most users, the Internet has been quietly evolving into a vast un-indexed data store. As a result, this Deep Web is so mind-bogglingly huge – some say more than 5,000 times the size of the Surface Internet – that it is both easy to get lost and to stay hidden.

Within this Deep Web are an unknown number of hidden networks; one of which is Tor, a dark world of anonymity. Here, people may communicate secretly and securely away from the attention of governments and corporations, scrutinize top secret papers before WikiLeaks gets them, and discuss all manner of unconventional topics.

Ironically, Tor – which stands for The Onion Router – was set up with funds from the US Navy at the start of the Millennium as a means of covert communication, and later to aid human rights activists inside repressive regimes. But so dark and murky is it, that other agencies now use it, as do most serious criminals.

Tor has its own websites, chat rooms, forums, blogs, file hosts, social networks and other features of the Surface Web. It is very easy to run into arms dealers, drug cartels, spies, pedophiles, kidnappers, slave traders and terrorists. You can buy top grade marijuana direct from the grower, trade stolen credit cards, buy the names and addresses of rape victims, or arrange the murder of an inquisitive reporter or pernickety judge – and then pay for it all with the Deep Web's own currency, the untraceable BitCoin.

Generally, this is why the Deep Web has a bad reputation. But it has positive aspects, too. There are many journalists who use Deep Web tools to communicate securely with whistle blowers and dissidents. Aid agencies use the same techniques to keep their staff safe inside of authoritarian regimes.

The Deep Web is also a largely-unknown research and information resource, a goldmine of knowledge lodged in the databases of academic institutions, small businesses and corporations, research establishments, galleries and governments. If you know the right entry points, you can mine a rich seam of multimedia files, images, software and documents that you cannot find on the Surface Web.

How Intelligence Gathering Works

While some people believe the Internet has set them free, others fear we are all voluntarily plugged into the finest surveillance apparatus ever devised. But let's be clear about this: everything we do in the digital world is open to scrutiny by suspicious minds because that's the way intelligence agencies work. If they didn't make use of this amazing opportunity, they wouldn't be very good at their job.

All sophisticated security services monitor Internet traffic within their own countries. The US monitors *all* Internet traffic if it passes through US-owned 'processing services', which the bulk of it does. Legally, just the bare bones of the communications are monitored – the who sent what and when. But, although they may not be open about this, many agencies are now looking directly into the message itself, looking for the expected and the unexpected in all our online communications and activities.

But don't suppose actual agents are used for such mundane tasks. Algorithms of stunning complexity analyze literally every word. And, when certain triggers are pulled, the surveillance moves up a notch and so on until it enters the physical world.

According to the US Government Accountability Office, back in 2004 there were 199 separate data mining programs being run by 16 Federal agencies on the look-out for suspicious activity.

By 2010, *The Washington Post* concluded after a two-year investigation that there were around 1,200 government agencies and 1,900 private companies working on counter-terrorism, homeland security and other domestic intelligence programs from within thousands of secret data processing sites and "fusion centers" that constitute an "alternative geography of the United States".

According to the US government's most recent figures, 4.8 million people now have security clearance that allows them to access all kinds of personal information, while 1.4 million people have Top Secret clearance.

The National Security Agency intercepts and stores the data from over 2 billion emails and other communications each day in its attempts to predict wrong-doing in what it terms the "paradigm of prevention" or "predictive policing"; and each day more than 1,600 people have their names added to the FBI's terrorism watchlist.

The US National Counterterrorism Center collects information on *every* US citizen and mines it for terrorism indicators. It then passes on much of this data to other government agencies and increasingly to corporations like Lockheed Martin, Raytheon, CenturyLink and AT&T.

Agencies like the CIA collect all the data they can and then they store it indefinitely. If they ever need to join the dots, it helps to have all the dots from the past to draw upon.

Journalists are especially interesting. They have contact with politicians and activists, they have their finger on the pulse and they are capable of causing all kinds of trouble both to governments and to corporations. If they become interested in you, they will monitor all your online activities and read your email. They will see who your contacts are and they will start to monitor them, too.

Tracking people in cyberspace is child's play, especially when more than half of all Internet users have a page on Facebook. Big Data – Social, Mobile and Cloud – has altered the flow of information, overtaking traditional media. With commercially-available software like Raytheon's social media data mining tool RIOT, simply enter a person's name and up pops a colorful graph showing where they have been, who they met and what they all look like. It then predicts their future movements.

If they have someone in their sights, the bad guys then insert malware into the smartphone or computer and take remote control; listening in on conversations, intercepting SMS and VoIP calls, and noting everything.

Nothing escapes their attention. There is a school of thought that the most successful companies got where they are today with a little outside help.

Imagine starting a service where millions of people will openly detail their lives and speak their minds. Then imagine being approached by an organization that would like to help you become a global brand. All you have to do in return is add a 'backdoor' allowing them direct access to the real names, physical addresses and activity logs of everybody who signs up.

If you don't play ball, well, your business will go nowhere and you might find that suddenly your credit cards don't work and then things begin to spiral downwards for you. It's not really an option. You build a backdoor. That's the theory.

When Briton Leigh Van Bryan, 26, planned a vacation to Hollywood, he tweeted friends that he intended to "destroy America", meaning in London-slang that he was going to have a jolly good time. The Department of Homeland Security didn't see it that way and were ready and waiting for him when he landed at Los Angeles Airport. He was handcuffed, interrogated for hours, locked in the cells overnight and unceremoniously deported.

They knew everything about him except what he was actually talking about. Algorithms may be smart but they just don't get the nuances. It's the little things like this which can set a suspicious mind off on a very deep investigation or drag you quickly off to a window-less cell.

It's the same with email. If you don't believe that every word you write is scrutinized, try typing into an email the words, *bomb kill Obama Tuesday* and see how long it takes for them to come and get you.

The emails you receive can be equally dangerous. Anything that contains an image or link in HTML format, not to mention attachments, could result in a tracking device, key-logger or a beacon being inserted into your device, alerting the sender to your presence and precisely where you are sitting at that very moment.

Trackers are everywhere. Pay a visit to Twitter or Facebook and they will instantly plant little robots that follow you around, noting everything you do. The FBI were recently caught planting trackers in a survivalist website to keep tabs on visitors, noting how much they spend on dry goods, which firearms turn them on and what they say in chat rooms.

To scoop up everybody else, the agencies channel users through a series of ‘black boxes’ or inspection points scattered around the net which then read everything that passes through them, analyzing it, logging it, storing it for deeper examination, or marking it for further attention.

With this so-called Deep Packet Inspection (DPI), all Internet traffic can be read, copied or modified, as can websites. DPI can also see who is uploading or downloading, what is inside and who is looking for it. Websites can be blocked and so can specific items within sites such as a particular video on YouTube.

Russia recently authorized DPI, ostensibly to trap pedophiles and prevent terrorist attacks, but some fear with the added ability to delve deep into its citizens’ emails and watch everything they do online.

When Iceland recently announced a ban on all Internet pornography, it set its hopes on DPI. But many also fear that the laudable aim of safeguarding children might just as easily be turned to suppressing internal dissent or to tracking down tax-dodgers in straightened financial times.

Generally, ISPs and most governments can examine the ‘header’ of a message, seeing where it came from and where it’s going, but they have not been able legally to peer inside. DPI has been used for years in the commercial world but only Tunisia, China, Iran and Kazakhstan legally use the system to curb dissidents.

However, under the Foreign Intelligence Surveillance Act, the NSA and FBI are legally able to tap directly into the servers of any US Internet company and one of the best ways to do that is with DPI. Under the PRISM program, the NSA is apparently able to access the servers of at least nine leading US providers, including Google, Facebook and Microsoft. The companies themselves would not necessarily know that they had been compromised.

But this is small-fry. The US – along with its Five Eyes cyber-partners Britain, Canada, Australia and New Zealand – taps directly into undersea and fiber optic cables as well as communications satellites, taking the data from the source. The result is that virtually everything which travels on the Surface Internet, and much else, is open to inspection.

Very soon, the Community Comprehensive National Cybersecurity Initiative Data Center in Utah, code-named Bumblehive, will be on-stream, capturing all communication globally, including the complete contents of private emails, cell phone calls and Internet searches, plus all the personal data trails from parking receipts, bank transfers, travel itineraries and bookstore purchases. Another NSA data facility is already under construction in Maryland.

Data storage is remarkably cheap and getting cheaper every year. Analyzing and storing it all is now a cost-effective reality and, once again, they would be failing as intelligence agencies if they didn’t. The CIA proudly admits that “it is nearly within our grasp to compute on all human generated information.”

Today everything is connected, everything communicates and everything is a sensor. Technology is moving so fast that even the major agencies can't keep up. Put all these things together and the inanimate becomes sentient and capable of decision-making. Suddenly the great dystopian fear is a reality.

And this is how they profile us all. It's been happening for years in the commercial world. Only when you appear to step out of line, say the wrong thing or spend too long looking at a bad kind of wiki, will you become interesting to the suspicious minds.

But mistakes are easily made in a world overseen by computers and not so easily rectified, as Mikey Hicks of New Jersey knows well. Every time he tries to fly, he is detained and thoroughly searched. Mikey is 11 years old and has been on an Airline Watch List since he was two.

As it turns out, the bad guys don't say *kill* or *bomb* in their emails or on Twitter. The terrorists and super-criminals can also hire the smartest brains in the IT world and they pay better.

According to the US National Academy of Sciences, whilst data mining may work in the commercial world, it simply isn't feasible to prevent atrocities because terrorists don't use a one size fits all model; they change and adapt their *modus operandi* as they go along, preventing the algorithms from picking out a pattern.

Curiously, governments and intelligence agencies know this, too.

How this affects Journalists

All journalists should be aware of the dangers they face in the digital world – the emerging battleground.

A reporter working on a story about a local man with an idea to counter IEDs (improvised explosive devices) would very likely read up on military statistics, watch a few explosions on YouTube, check out the different detonators and view an extremist website or two. He would be asking for trouble.

From that day on, the reporter would be a marked man or woman. They could no longer research in private or correspond in confidence. They would never be able to protect the anonymity of a source.

What they could have done, however, was install a few free, tried and tested programs and tweak their computer and smartphone. They could easily have masked their identity and location. And they could ask questions without Google or the NSA building a profile on them.

But it is not just intelligence agencies and law enforcement that we should worry about. All kinds of people have a vested interest in knowing about your next story – individual criminals and criminal organizations, political parties and extremist groups, law firms and the corporate giants.

Large business interests have their own intelligence units. They know what is being said about them and by whom. They keep track of their competitors and they know when somebody starts asking awkward questions about them.

If big business wanted to destroy a journalist’s reputation this is simplicity itself. It would be a small matter to fill the reporter’s computer with images of child sexual abuse and then tip off the local police anonymously. No one would ever take the reporter seriously again. Even their closest friends and family would turn against them.

So be warned. The Internet is a dangerous place and there are people out there with high-end computer skills who can seriously damage your life.

The key is not to attract attention in the first place by learning to operate beneath the radar. But if you suspect you are being monitored there are ways and means of hiding your activities and communicating in ways that cannot be discovered or intercepted.

But it is also vitally important not to “go quite”. If you suspect you are being observed, you must carry on as you have always done. Continue buying cinema tickets online, chatting with your friends and posting to the social media, and all the rest of it.

When US Navy SEALS killed Osama bin Laden, they knew his was the only house in Abbottabad that did not have broadband or connect to any phone network. He did not have a Facebook page and he never tweeted his friends. And this is what gave him away.

So you must give them something to monitor. You need to keep them satisfied and to divert their attention while you operate elsewhere in unexpected ways.

And, rather like spies in a James Bond movie, journalists have an array of digital tools to call upon, both to mask their identity and to provide real confidence that their correspondence, notes and contacts are secure.

There are smartphone apps that let you see in the dark or measure the height of a building. You can film and record without being rumbled; send emails, Private Messages and SMS text messages that cannot be intercepted or read.

With any modern device you can access banned websites and take over and control public and private security cameras. You can continue tweeting when the authorities take down Twitter locally. You can pass on and store documents away from prying eyes. You might even hide news footage of a massacre inside a music track on your iPod while you slip across the border.

In the old East Germany under the Stasi Secret Police people didn’t talk openly because they didn’t know who was listening. And now we have the same situation on the Internet. And the ability to speak openly was one of the best things about the Internet. In many ways – with their suspicious minds – they’ve ruined something that was truly marvellous.

So, will people speak openly if they know they’re being monitored? Is this likely to have an effect on the free flow of thought and ideas? The answer can only be “Yes”.

In short, free democratic society is threatened by this mass surveillance. And the Press – as the cornerstone of democracy – has never been so threatened before.

It’s time to wake up to the Internet and to see it as the 21st century battleground where, in many ways, we’re all combatants.

And, for the first time, we’re combatants in a war not simply observers – not simply trying to get at the truth but actual targets in the sights of “democratic” governments and not just those of the repressive regimes, those that have traditionally tried to silence the Press and stamp on the Human Spirit.

The Internet may be an amazing tool. But, if we don’t learn to master it, it may be the end of us all. Because, if we can’t work in private and offer confidentiality we are compromised.

Then what future this profession?

A technical aside

We are living in a constantly-changing game of cat and mouse. Techniques that might work today might not work tomorrow.

In the brief period since this book was first published, a number of groups offering cyber-security and counter-surveillance technology have been forced out of business or outright compromised.

We endeavor to keep this book as up-to-date as possible. If, however, you find that any of the techniques offered here are no longer valid, please let us know as soon as possible so we can launch an update. Equally, we recommend that you register for free updates below.

Depending on the format of this book, all of the links given here should open in your browser. Deep Web links marked <!> can only be opened in a Tor-Firefox browser, which you will learn to configure later.

This book generally concerns itself with the Windows operating system because this is the most popular world-wide. However, where applicable, instructions for Mac and Linux systems are also given.

Anyone using the latest Windows 7 or 8 64-bit machines may have trouble installing some of the free software out there because Microsoft, to ensure you use its products, has made this very difficult. Where possible, other options or work-arounds are given.

Free, open source software is generally preferable to the paid-for variety because it can be tested by developers and any logging devices or backdoors can be identified. All proprietary encryption software should be treated with the upmost caution.

Be alert that no single system or piece of software is 100% secure or safe. However, by combining the techniques in the following pages, it is possible to operate in such a way that nobody ever need know.

PART 1 - Security

If you are conducting sensitive research or just your normal day-to-day activities, it is advisable to make a few, simple adjustments to your computer.

Setting up Defenses

Browser — arguably the most security-conscious browser is Mozilla Firefox which has a large number of free add-ons to help you beef up security. You can switch between regular and private browsing by clicking the Firefox logo in the top, left-hand corner. This will prevent your computer from logging your activities but it will not make you invisible.

Spend a minute or two tweaking with the *Settings*.

> Click the Firefox logo and select *Options/Options.*
>
> In the dialog box, open *Privacy* then tick the option *Tell websites I do not want to be tracked*. There is an option to *Always use Private Browsing mode.* Untick *Accept cookies from sites*. Tick *Clear history when Firefox closes*. Under *History* select *Use custom settings for history* and select *Never remember history*.
>
> Under *Security*, tick *Warn me when sites try to install add-ons*. Remove all exceptions. Tick *Block reported attack sites*. Tick *Block reported web forgeries*. Untick *Remember passwords for sites*.
>
> On the *Advanced* tab, under *General* tick *Warn me when websites try to redirect or reload the page*. Under *Network* tick *Tell me when a website asks to store data for offline use*. Tick *Override automatic cache management* or set Cache Size to 0.

Force HTTPS — Hypertext Transfer Protocol Secure (HTTPS) is used for secure end-to-end communication. HTTPS Finder for Firefox automatically detects and enforces HTTPS connections when available, providing a reasonable guarantee that you are communicating with the intended website and not an imposter, plus ensuring that communications between the user and site cannot be read or forged by a third party. The Electronic Frontier Foundation has its own free version HTTPS Everywhere for both Firefox and Chrome browsers.

Kill Trackers — Do Not Track Me blocks web beacons and trackers that monitor browsing habits. Once installed, a tiny icon in the top right corner of Firefox issues an alert whenever a site has a bead on you. Twitter and Facebook, for example, will try to insert trackers that follow you all over the Internet, allowing them to build a detail profile of your movements and interests. If people ever wonder how the social networks make money, this is how. To see just who has a commercial interest in what you do online, DNT+ publish a comprehensive list of the companies involved, together with information on them.

Control Cookies — BetterPrivacy allows you to remove or manage cookies and gives various ways to handle Flash-cookies set by Google, YouTube, eBay and others. Privacy+ does much the same thing. Flash plugins run independently of your browser and bypass any proxy configurations. If you were trying to mask your identity, these will reveal your IP address which in turn will point to your physical address.

Java Switch — QuickJava allows you to quickly enable and disable Java, JavaScript and other intrusive plugins which track your travels and preferences. Other options include NoScript and Ghostery.

Cache Control — the Empty Cache Button adds a button to Firefox allowing you to quickly empty your browser cache should anyone start looking over your shoulder and optionally reload your page with just one click.

Password Protect — KeeFox is a simple and secure password management plugin for Firefox.

Avoid Detours — to stop websites opening other pages on your browser and taking you off to potentially harmful sites, try Redirect Remover which prevents redirects from links and images. Another good option is RequestPolicy.

Control Ads — Adblock Plus allows you to block on-line ads from anyone you would rather not hear from. You can choose from a predefined list and you can personalize your own, but don't block sites you use regularly. Amazon, for example, is so stuffed with ads that by switching them off, the site instantly turns to text-only. You can also customize the settings to remove the annoying ads at the beginning of streaming videos on YouTube and elsewhere.

Block Baddies — use either the free or paid-for versions of AVG or Avast which both warn of and block viruses and spyware entering your machine from malicious websites (see Keeping out the Spies).

Secure Download — DownThemAll uses the FireFox safety settings and so requires no configuration and features an advanced accelerator that speeds things up considerably. You can pause and resume downloads. It also allows you to download all the links or images on a webpage and customize the search criteria. It offers the ability to download a file from different servers at the same time for additional security. Privoxy is a web proxy service that fetches items (webpages, images, movies, etc) and passes them on to you when complete.

Encrypt — Encrypted Communication encrypts messages prior to transmission, including posts to Facebook and other social networks, and is simpler than many other encryption options.

Search Engines — obviously, Google keeps detailed records of your search queries so select an engine which won't store your records. Options include the Secret Search Labs engine and iXQuick.

Tighten Router — change the password on the home or office router to prevent unauthorized access.

Wear a Mask — you can't beat cloaking your identity as one of the safest of all strategies. This way no one need know who or where you are. The simplest solution for quick, anonymous browsing is to use a facility such as AllNetTools, Guardster or Anonymouse. These free services allow you to type in any web address and then travel around without leaving a trace of your activities or giving away your location. These are particularly useful for sensitive search engines queries and for visiting locally banned websites.

You can set up a proxy – which gives the impression that you are in another place – by fiddling with the *Settings* in Firefox and changing the IP address to one provided by Proxy4Free or Rosinstruments but this can slow your machine down. A simpler solution is Stealthy, a Firefox add-on which seeks out the fastest proxies available and automatically routes you through them.

A very good and more secure alternative is a Virtual Private Network (VPN), effectively a 'secret tunnel' where all your on-line activities are screened from the service provider and eavesdroppers. Free versions include FreeVPN and ProXPN. A popular and fast paid-for option is VrprVPN.

Regularly backup all data, either to a separate storage device or to a Cloud service you can trust, such as those run by Trend Micro and Avast.

If it's not too late, never post any personal information – birth dates, family connections, location, travel plans, identifying photographs, etc – on the social networks. To tighten Facebook privacy setting, see the online guide by Trend Micro.

All this is good for general activity on the Surface Web but it is not 100% secure.

It is safe to assume that if law enforcement or the intelligence agencies want to monitor anybody's Internet access – read their emails and social media postings, harvest their contacts, find out what they are searching for and downloading, and listen in to their calls – then they can, regardless of the niceties of court orders and warrants. This means that absolutely everything is open to inspection.

In the final scene of the movie "Raiders of the Lost Ark", they place the Ark of the Covenant inside a crate and then they hide it inside a humungous warehouse full of identical crates. This is the principle by which to operate, but on an infinitely vaster scale – down in the Deep Web.

1.2 Accessing Hidden Networks

Tell someone that you know how to go off-radar on the Internet and as a rule they won’t believe you. They imagine the intelligence agencies have state-of-the-art technology and can see everything you do. This is only partially true. They do have amazing technology but they can only see things if they know where to look. Down in the Deep Web, by mixing and matching different technologies, you can stay out of sight and make it seriously difficult for any adversary to locate you.

There are several hidden networks. There may be hundreds but nobody knows for sure. We are going to access the most user-friendly – Tor.

First you need a specially-configured web browser to divert your traffic through a worldwide volunteer network of servers. This conceals your location and your activities, effectively hiding you among all the other users. Tor works by encrypting and re-encrypting data multiple times as it passes through successive relays. This way the data cannot be unscrambled in transit.

Tor does have its flaws and should not be considered completely safe. Although your IP address is concealed, a digital fingerprint can linger allowing someone accessing your local network – a Wi-Fi provider or an ISP working with criminals or law enforcement – to glean some idea of your activities.

However, the waters can be muddied for any eavesdropper by requesting more than one site at a time or by downloading more than one item simultaneously, and by regularly re-setting the *Use a new identity* facility on the Tor control panel.

Certain plug-ins will not work on the Tor browser such as Flash, RealPlayer and QuickTime as they can be manipulated into revealing an IP address.

Begin by downloading the free Tor/Firefox bundle. This is safe and easy to install. Simply follow the on-screen instructions and a gateway to the Deep Web can be configured in minutes with no special skills.

Be absolutely certain that you are downloading from the torproject.org website. A hidden network used in Iran was recently infiltrated when a fake version of their modified browser was distributed which gave away the identity of users. Also be sure to keep the Tor browser up-to-date by regularly checking for the latest version. Also, add an HTTPS enforcer, such as HTTPS Finder or HTTPS Everywhere.

Once loaded, the browser will display a very basic-looking webpage (the Deep Web resembles the Surface Web circa 1996) and the words:

Congratulations. Your browser is configured to use Tor.

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.

Where is says ‘*Your IP address appears to be…*’ are a set of numbers that in no way connect to your computer. You are now anonymous and free to explore Tor or branch off to the Surface Web with minimal risk of being monitored.

If you are in a country where ISPs or the government block the Tor network, open *Settings* on the Tor control panel, select *Network*, and then tick the box *My ISP blocks connections to the Tor network*. You are now given the option to *Add a Bridge* or *Find Bridge Now*. If no bridges (non-public relays) are found, go to the Tor bridge relay page on the Surface Web and select them manually by cutting and pasting until you find one that works for you. Add as many bridges as possible as this increases your chances of connecting and improves security.

Using Tor

Rather like time travel, this level of the Internet appears much as it did in the very early days, including the lengthy wait while pages load. There are no frills or flashy graphics, just simple text and images.

On Tor, people communicate secretly and securely. Whistle blowers and dissidents, activists and journalists, aid-workers and academics, criminals and terrorists, and rather a lot of librarians, all carry on their day-to-day activities.

Top secret papers are posted here, as are guides and wikis for every type of activity, legal and otherwise; and all manner of unconventional views are expressed. Here you can lurk hidden and surreptitiously store any amount of data for free.

This is pioneer territory with very few settlers; perhaps 400,000 daily users at best compared to the 2 billion plus who stay up top. Some of the natives are hostile because they would rather keep the place to themselves. Others are friendly because they know more users mean more people to hide amongst.

Deep Websites can disappear or fail to load from time to time. If you have difficulty opening a particular page, just try again later and it may reappear. Deep Website availability can be checked at *Is it up?* <!> http://zw3crggtadila2sg.onion/downornot/

Entry Points

The Hidden Wiki <!> http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page — often described as the hub of the Deep Web, this is the best starting point for new-comers. Here you can find lists of other hidden networks and links to black market goods and financial services, file hosts, blogs, forums, political groups and whistle-blowing boards. The wiki is available in 17 languages.

Tor*Dir* <!> dppmfxaacucguzpc.onion — simple gateway into the Tor network broken down into categories, such as *Activism, Libraries, File Sharing, Blogs, Security, Adult, Gambling*, etc. At the top of the page is a search facility.

Tor*Links* <!> torlinkbgs6aabns.onion — links directory where you can add your own links and set up a Deep Website.

Tor*Help* Forum <!> http://zntpwh6qmsbvek6p.onion/forum/ — help on Tor and Hidden Service setup and configuration.