Volume 2, Issue 1 OCTAVIAN REPORT March 2016

IN TOO DEEP: THE DARK WEB AND ITS DENIZENS

BY **DEE SMITH**

The Internet is a strange and unknown place — and much of it lies far beyond the scope of normal users. The so-called dark web is one such digital wilderness. Almost anything can be found for sale there, from guns to drugs to hackers-for-rent. The dark web's existence raises a whole host of risk issues. The most pressing are on the national-security front, as governments battle cyber attacks possibly launched from the dark web's depths. Dee Smith helps you make sense of it all with this disturbing analysis.

If you are like most people, what you access on the web is merely one layer on the surface of what is really out there. What you can reach with an ordinary commercial web browser is less than 20 percent of the Internet. But with the right tools and the right skills, you could enter the dark web, which best guesses estimate represents some 81 percent of the Internet. This is the domain of hackers and terrorists, dealers in the illicit, traders of everything from cyber weapons to child pornography and almost anything else imaginable.

Think of the Internet as a layer cake. What ordinary users access intentionally is the cake's fairly thick layer of icing. Below that are other layers sometimes called the "deep web." Without realizing it, people access the deep web very frequently. Buying a plane ticket, ordering something from Amazon, or signing up for medical insurance: all involve accessing the deep web. This normally invisible area comprises, among other things, the parts of the Internet that house, control, and process the databases that enable those kinds of transactions. In theory, they are secured from unauthorized access. But as we all know, that security is often very weak in practice. The so-called dark web is a special part of the deep web. Think of it as the bottom layer of the cake, where things are particularly inaccessible unless you know exactly how to reach them.

That metaphor is a gross simplification, of course. The Internet is not anything like a layer cake. It is a network of processors, of which your computer, your phone, and in some cases your car, thermostat, and refrigerator are parts. It is a network of unimaginable complexity, and no one has mapped it in meaningful detail. The bulk of it was built over only the last two decades; current estimates show that human society globally now generates as much information every day as it did from the dawn of civilization up to the year 2000. Many of the systems processing all that information constitute the so-called deep web; the dark web, part of the deep web, can only be accessed by means outside the experience of most Internet users. Primary among these are deep web browsers, of which Tor is the best known. It is important to understand that you cannot get on the dark web unless you are anonymous. Anonymity is more than part and parcel of the dark web: it is built into its fundamental

fabric.

Unsurprisingly, minuscule exposure, technical sophistication, and anonymity have combined to create a system that thrives in parallel to the open Internet. A great deal of the activity taking place there is — as in its open counterpart — commercial. But it is a commerce in commodities that could never be bought or sold on the open Internet. You can order marijuana or heroin to be shipped by mail and can pay for your order using cryptocurrencies such as Bitcoin, an anonymous payment system based on block chain technology, where a "public" ledger replaces a trusted third party such as a bank.

But recreational drugs are perhaps the least disturbing items available via the dark web. Snuff films, child pornography, stolen credit-card data and other personal identity information, even human substances like saliva, organs, and other biologicals: all come into the marketplace. Contract killers offer their services, complete with pricing on targets ranging from civilians to political leaders. A site called White Wolves Professionals has offered services ranging from the murder of a "Citizen" for $25,000 (presumably U.S. dollars), to that of a "CEO Company" for $250,000, to the assassination of a "Hight politican" for $15,000,000. They require a 50 percent deposit in cash. Another offer, from someone called "fritz," is priced at €100,000 for a "High rank government official." A service called "C'thulhu (a literary reference to the chief god within the pantheon created by fantasy writer H. P. Lovecraft in the 1920s) offered a long disclaimer about risk, advising that those not ready to take risks should not contact "this kind of organizations" [all sic]. Bad grammar and faulty punctuation may lend such offers an eerily comic air, but that doesn't mean anyone can discount them entirely.

Other criminal entrepreneurs can be found in these precincts as well. Theft, done by (supposed) professionals, is for sale. An entrepreneur called Dangler has offered not only to steal on order, but also to sell the user items he has already stolen. These range from expensive toys to expensive clothes. There are even offers to sell human slaves. A site called Black Death was reported to have women for sale with opening bids of $150,000, but the reality of at least some of the individuals was later called into question. Weapons of all kinds are for sale. This includes malware and the services needed to deploy it. Sites like "Rent-a-Hacker" have offered the services of a professional hacker to "solve your problems, destroy your enemys" [sic]. An organization or even an individual with only relatively modest means can hire the talent to mount a fairly devastating cyber penetration, whether to steal data or to disrupt.

Much of the talent operating in this environment is very young, and large, less-agile entities like companies and governments have difficulty competing (although they do in fact hire such talent, for both white-hat and black-hat work). In addition to hacking, there are several new services available through the dark web. Document exploitation (or docex) is an emerging trend: manipulating data in situ rather than stealing it. Encryption capabilities are also sold on the dark web, and these are providing a mounting challenge to governments. End-to-end encryption, if done well, can make the encrypted data essentially inaccessible to others in any feasible time frame. This could change if workable quantum computing arises, but for the moment the computer power necessary to crack hard encryption means it can be done only very selectively.

This is particularly important when it comes to the information-sharing that occurs within the criminal groups, terrorist groups, and others operating in the dark web who seek to disrupt the powers-that-be. The extent to which such sharing occurs, even among groups with no other links, is not generally appreciated. New hacking techniques and other information are disseminated quickly and widely by the bad actors in the dark web. This is in stark contrast to the lack of information-sharing that occurs among good actors — even those who are allies. The central reason for this is that governments, and in particular their law enforcement and intelligence agencies, operate with a culture centered on a "need-to-know" basis.

There is a long-standing disposition against sharing information because it would compromise sources, methods, and tradecraft, devaluing the information and making it less actionable or usable. Unfortunately, the willingness of the bad actors to share much more freely puts their counterparts continually behind the proverbial eight-ball. It is hard to see how this can or will be addressed, given the fact that various agencies even within the same government often fundamentally resist sharing information.

> "Why do the powers-that-be allow the dark web to persist? Why not shut the whole thing down?"
>
> —*Dee Smith*

So why do the powers-that-be allow the dark web to persist? Why not shut the whole thing down? There's the issue of difficulty. Something so amorphous and well-hidden has a certain amount of protection ipso facto. Nevertheless, as the Tor system (also known as the Onion) was originally designed by the U.S. Navy, it would probably be feasible for the U.S. government to shut it down or at least severely hamper it. Another reason may be more important here: covert utility. The governments of the world are down in the dark web, too, gathering intelligence on enemies, conducting counterintelligence operations, false flag operations, and other activities — including mounting attacks on their foes. All countries can now in theory provide themselves with cyber attack capability, because they can simply buy it on the dark web. Easy to chuckle at, perhaps, until you recall that a single, skilled hacker can do a huge amount of damage. Our ADA electrical power grid system — ADA stands for advanced distribution automation, which refers to the mechanisms and protocols by which the regulation of load and distribution of power takes place — is old and vulnerable. It was not designed to handle the loads it is now required to, and could be disabled by the right kind of cyber attack. One that might very easily be contracted for and provisioned in the dark web. And that is only one example of many. Docex, described above, also has anti-state as well as civilian criminal uses. Imagine the damage changing certain documents with sensitive information in them could cause (consider changing inventories of critical materials or weapons, for example, or rewriting part of the code that controls a single nuclear power plant), particularly if it is done capably enough that no electronic copy of the original information exits.

A study published in February by King's College London found that 57 percent of the dark web is used for "illegal" activities (and the study's authors note that this is a conservative figure). However, such illegalities included the use of the dark web to access sites like Facebook in oppressive countries where open access is illegal. In fact, such activities would constitute "anti-state" uses of the dark web, but against repressive states.

There have been attempts to shut down pernicious parts of the dark web. Consider Silk Road, a black marketplace launched in 2011, where the kinds of things listed above and many others were traded. It was shut down by the FBI in 2013 and its alleged founder was arrested. But since Silk Road was shut down, similar marketplace sites have launched, including one called Silk Road Reloaded. Such platforms continue to launch, are sometimes shut down, and then replaced in turn by newer platforms.

In the context of the ironic dichotomy between the desire for greater privacy on the one hand and the desire for greater security on the other, some activities being conducted or under consideration by liberal Western democratic governments may ultimately drive more of their citizens to use the dark web for non-criminal purposes. The Investigatory Powers Bill,

currently making its way through Britain's parliament, would require communications service providers to keep the metadata of users for 12 months. Tor, however, anonymizes metadata, so that it is not attached to individuals. Although people with

nothing to hide may not need to hide anything, there is nevertheless a growing global distrust of governments and a concomitant desire to avoid scrutiny on principle.

So the dark web can be a sinister place. But as long as major powers — and those who wish to avoid the increasing reach of their surveillance — find it more useful than not, it will continue to thrive.

Dee Smith is the founder and CEO of Strategic Insight Group.