Tangled web

Law enforcement struggles to control darknet

Operation Onymous has shut down numerous darknet markets, but advanced privacy and decentralised systems pose challenges to combating new illicit trades online. Rodrigo Bijou analyses whether law enforcement efforts can keep up with technology.

Key points

- Darknet markets have multiplied since the first major takedowns in 2013, and continue to use advanced privacy and decentralisation technologies that have so far frustrated law enforcement efforts.
- An exclusively interdiction-based approach to darknet markets is limited in its abilities to deter cybercrime on the darknet, and may be politically precarious as privacy advocates will continue to criticise any circumvention of technologies that political activists and others depend on.
- The same technologies, including Bitcoin, upon which illicit darknet markets are built, have attracted significant venture capital, and this is likely to have an impact on political and law enforcement bureaucracies seeking progressive opportunities to tax and control the darknet.

An international law enforcement operation in early November, dubbed Operation Onymous, successfully took down more than 400 hidden sites operating on the so-called 'darknet', the hidden part of the internet inaccessible to normal search engines. The agencies involved, including the US Federal Bureau of Investigation (FBI) and Europol, conducted months of surveillance in order to shut down these sites as part of a larger effort to combat the burgeoning flow of illicit goods and services through established forums and marketplaces accessible online.

The darknet sites targeted in Operation Onymous and others that have been seized by law enforcement in the past few years are primarily hidden marketplaces only accessible through The Onion Router (Tor) browser and network. The anonymity of the identities of administrators, vendors, and buyers is ensured through the use of encryption tools such as Pretty Good Privacy (PGP) and the Tor browser. These safely ensure a private connection to the site, secure transactions, and anonymous, but verified, communication between buyers and sellers.

The illicit wares in question range from traditional, physical goods such as cocaine and small-arms, to mercenary hacking services and stolen credit card numbers sold in bulk. The internet has long had an underground of illicit transactions, and many tools involved such as PGP and Tor have been in existence for years. However, recent dark market activity has surged with the advent of new cryptocurrencies such as Bitcoin that have systematically decentralised payment processing and made it entirely anonymous.

The tools and guides to connect to these sites, encrypt communications, or buy cryptocurrency are freely available on the open internet to download, and in some cases have been repurposed for illicit activity from initially unlikely development. Today, the tools are most often used to connect to a thriving, well-organised collection of marketplaces where everything from black tar heroin to automatic weapons are sold openly, and shipped globally, to any willing buyer.

The marketplaces that have been targeted by law enforcement span completely open models to those specialising in certain regions, languages, or goods. For example, some marketplaces such as the Russian Anonymous Marketplace (RAMP) ban goods and services such as child pornography or hacking that draw more law enforcement attention than drugs or stolen credit cards.

Troels Oerting, assistant director of Europol and head of its European Cybercrime Centre (EC3), told *IHS Jane's* on 19 December, "We have lately seen a large amount of physical crime move online, at least the 'marketing' and delivery part of the business... [Buyers can] get the illegal commodity delivered risk-free to a place of their choice by the mailman or a courier, or maybe by drone in the future, and can pay with virtual currency and in full anonymity, without the police being able to identify either the buyer or the seller."

Since the first wave of major markets such as the Silk Road began in 2011, virtually all markets now include advanced reputation, search, and shipping features, similar to legitimate online marketplaces such as Amazon. However, considering the nature of the goods and services sold, these features are extended alongside forced encrypted messaging and secure connections to mitigate risk for buyers, sellers, and market administrators. As the illicit online economy has matured, an

ecosystem of services that mirror legitimate shopping online, such as affiliate advertising networks, has also sprung up alongside more criminal offerings such as automated money laundering and mercenary hacking services.

The law enforcement efforts to take down sites in Operation Onymous mark the latest interdiction attempt to combat illicit activity on darknet sites, which has been on the rise since the founding of the first Silk Road market in February 2011. However, illicit online activity, advances in the technology that powers its anonymity and security, and often ill-fated law enforcement attempts to interdict these actors date back decades earlier.

Silk Road and before

Since the late 1980s, when cellular and internet technologies began to be adopted commercially and criminally, the separation of digital and physical criminal activity, and the ability to deter that activity online, has challenged law enforcement agencies to increase their operational tempo and expertise to match the pace of innovation. Initially, countries known as tax havens, or those still in a legal state of flux after the Cold War, also began to offer their space as a secure, digital "data haven" for online activities including gambling, pornography, and in some cases a free rein for hacking.

As criminal organisations, and more importantly average home users, began to conduct more activities online, new peer-to-peer networks for securely sharing content, in particular copyrighted media, began to form. Countries that have been havens for cyber-crime, in particular former Soviet Bloc countries and China, are minor in comparison to the complex, globally distributed networks powering the darknet and its predecessors.

Conducted in the open internet, or "clearnet", platforms such as Napster and Limewire marked the first major advances for everyday, average users being able to intuitively, and securely, trade information. These technologies, and later iterations of decentralised communications such as BitTorrent and Bitcoin, made progress towards a fully anonymous, cryptographically secure way to communicate data online.

Although these technologies and the communities that sprang up around them were initially used mostly for illegal downloads of music or movies, they were later appropriated for a variety of purposes, including password-protected terrorist forums and the dark markets that have become increasingly popular since the late 2000s.

The tools such as Tor used to anonymously and securely access darknet sites have a longer history. Since the late 1990s, there have been tools aimed at creating decentralised, anonymous spaces on the internet such as Freenet, created in 2000 and described as a "censorship-resistant communication" platform, or the Invisible Internet Project, created in 2003 as a network layer that enables computer applications to send messages securely.

As these projects matured, the components for cryptographically secured, private communications could be pieced together with advances in anonymous currency, hosting, and payment processing to construct an end-to-end protected transaction for a buyer searching for illicit goods, finding listings, securely contacting anonymous vendors with encrypted shipping information, and finally totally anonymous payment processing.

One of the most common parts of this

Employees at the European Cybercrime Centre (EC3), at Europol headquarters in The Hague, Netherlands, on 11 January 2013. EC3 is at the forefront of global policing efforts to tackle criminality on the darknet.

PA: 1629089

Troels Oerting, head of the European Cybercrime Centre (EC3), on 11 January 2013. Oerting told *IHS Jane's* in December 2014 that there had been no decrease in the number of services being established on the darknet.

PA 1629087

end-to-end chain today is Tor. The platform was initially developed and first released in 2002 by the US Naval Research Laboratory, and was first conceptualised as a means of protecting dissidents in authoritarian nations such as China or for use by government agencies looking for a globally secure, and anonymous, communications solution.

Beyond Tor, the latest advance that has been widely adopted has been cryptocurrencies, which have enabled untraceable, yet publicly verified, payments online. First released in 2009 by a developer using the pseudonym Satoshi Nakamoto, Bitcoin was almost instantly adopted across the first major darknet markets such as the Farmer's Market and Silk Road as a more anonymous means of payment than money orders and cash.

The first wave of major markets that operated on this end-to-end anonymous model were an initial test for law enforcement, particularly in the case of Silk Road, which grew to be the most popular first-wave market with more than 10,000 listings of illicit goods and services. Even though the market began in February 2011, it took two years for the FBI to run surveillance and apprehend its creator, Ross William Ulbricht (aka 'the Dread Pirate Roberts'). Ulbricht's trial began on 13 January 2015, with charges against him including computer fraud, money laundering, and drug trafficking conspiracy. He has pleaded not guilty.

The figures listed in the federal indictment of Ulbricht were a nod to the growing popularity of darknet markets, with the Silk Road alone doing more than USD1.2 billion in sales between its inception in 2011 and takedown in 2013. Although this may be a small fraction of the global drugs trade, the implications of the darknet platforms for law enforcement and the overall economy are much larger.

After Onymous

Since the first major takedown in 2013, dozens more markets have been founded, including Silk Road 2.0 and newcomers such as Hydra that are a direct nod to the ability of darknet markets to proliferate as a few are eventually taken down by law enforcement.

The most recent of these takedown operations was Operation Onymous, conducted by Europol in conjunction with the FBI and several other agencies, which reportedly took down hundreds of hidden services. The numbers reported are slightly misleading at first glance, as although major markets such as Silk Road 2.0 and newcomers such as Cloud 9 were shut down, they represented a small portion of the sites taken down. The conflation between "hidden services" and darknet markets will be a significant indicator as operations continue, and agencies will be looking to portray signs of progress in deterring cyber-crime.

The growth in these markets, and subsequent difficulties faced by law enforcement in shutting them down, can be explained by the maturation of darknet market features and the increasingly advanced set of technologies that power them. Customer experience features including 'customer service teams' running special offers and vendor reputation systems similar to those on legitimate web stores such as Amazon or eBay are now standard across all markets.

These features have made buying everything from hacking services to club drugs online an easier, more appealing experience for average consumers. Customers can choose from shipping options including overnight by unwitting legitimate couriers such as UPS, sort through thousands of reviews for single vendors, and expect a package in the post as they would any other online purchase.

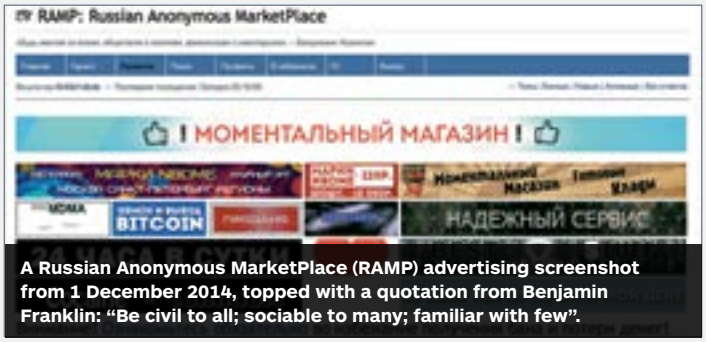
Yet the apparent importance of vendor reputation on many darknet sites is disputed by law enforcement agencies. Steve Welsh, the Head of Behavioural Science at the UK National Crime Agency (NCA), told *IHS Jane's* on 19 December, "It is important to highlight that, despite apparent customer satisfaction rating for vendors on dark web criminal markets, they are very much environments where people seek to mislead, cheat, and defraud others."

The other influential trend has been the development and adoption of more technical features such as multi-signature authentication and cryptocurrencies such as Bitcoin, which have made these purchases more difficult for law enforcement to disrupt or trace back to sellers and the platforms on which they operate online. Multi-signature authentication has advanced the security of market transactions, in which the marketplace will create a temporary "wallet" that requires the cryptographic keys from the buyer and vendor to release funds.

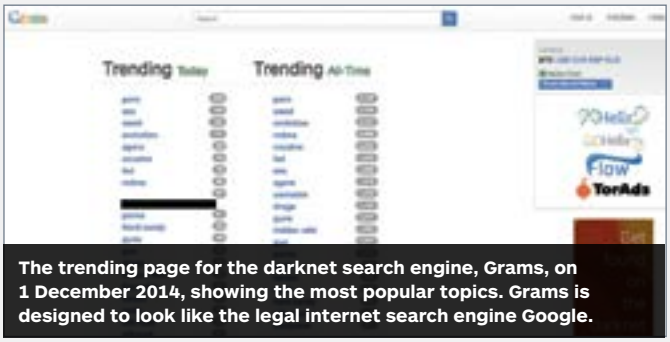
For a "normal" and licit transaction, this would mean a consumer, eBay, for example, and the vendor all providing a verified signature to release the final funds. This multi-party authentication makes stealing funds virtually impossible for other cyber-criminals, and more importantly makes tracking transactions and interdicting money even more difficult for law enforcement. Markets have made this entire process a point-and-click feature, shifting the asymmetric balance even further where new features mitigate risk between buyers and sellers, while making it more difficult for law enforcement to shut markets down or attribute transactions.

Cryptocurrencies such as Bitcoin, and the now dozens of variants including Litecoin

Screenshots from the darknet



A Russian Anonymous MarketPlace (RAMP) advertising screenshot from 1 December 2014, topped with a quotation from Benjamin Franklin: "Be civil to all; sociable to many; familiar with few".



The trending page for the darknet search engine, Grams, on 1 December 2014, showing the most popular topics. Grams is designed to look like the legal internet search engine Google.

Drugs for sale with purity and price information on the BlackBank site on 1 December 2014. Orders are shipped directly to customers using couriers.

An English translation from Russian of the 'house rules' for the RAMP site, on 1 December 2014.

The welcome screen that replaced Silk Road 2.0 following seizure of the market in Operation Onymous.

The BlackBank market homepage on 1 December 2014. In common with other darknet markets, BlackBank's model aims to create confidence between vendors and buyers.

Homepage of the Bitcoin Fog cryptocurrency trading site, used for money laundering, on 1 December 2014.

An AK-47 series assault rifle for sale on the Evolution darknet market, on 18 December 2014. Evolution benefited from the takedown of Silk Road 2.0 after Operation Onymous in late 2014, and is now the dominant marketplace on the darknet, followed by Agora and Nucleus.

Homepage for the TOM drugs darknet market on 1 December 2014. TOM is accessible only via the Tor network.

PA: 1572142

Officers from the UK National Crime Agency (NCA) on 7 October 2013. The NCA leads operations in the UK against online criminality. PA: 1629088

and Zetacoin, are also causing difficulties for law enforcement efforts online. These currencies are impossible to trace back to original owners, and cryptographically secured to exchange globally, at network speed.

The NCA's Welsh told *IHS Jane's*, "Payment methods are expanding, with the advent of virtual currencies beyond the likes of Bitcoin. We work on an ongoing basis to understand how criminals are using non-traditional methods of payment, and any opportunities this can present for law enforcement."

Consequently, law enforcement agencies are unable to use currency to tie together criminal networks and discover where major goods or services are being sold, or money laundered. These technological developments are what finally secured an end-to-end transaction chain from messaging to purchasing, which in turn enabled markets to mature to their current point of diminished risk of prosecution or surveillance.

Growing ecosystem

Just as the markets have matured with new features, an advanced ecosystem of services around illicit trade online – from search engines to money laundering – has grown in the burgeoning darknet economy. One popular new service is Grams, styling itself with an appropriated logo and mission as the 'Google' of shopping on the darknet. Grams indexes tens of thousands of listings across many darknet markets and allows consumers to openly search for drugs, weapons, pornography, or whatever they desire across multiple darknet markets.

On the transaction side, automated 'tumbling' (money laundering services) have sprung up that will randomly cycle Bitcoins or other cryptocurrencies through a variety of wallets, making transactions even more difficult to track. Similar to the marketing and technical features, this ecosystem of services around darknet markets has made it easier for consumers and harder for law enforcement. Consumers can easily search for listings and trust that their transactions are secure and anonymous, while law enforcement operations like transaction surveillance and taking down markets are more difficult.

Although the darknet itself has decades of history, the rapid rise in open markets for illicit goods online has presented new concerns for law enforcement in old and new crimes. In the first category, law enforcement faces greater obstacles in combating traditional crime such as drug or arms trafficking in a more globalised economy. For example, tracking small vendors in the United Kingdom who use decentralised, hidden services, and who sell to a global population, is incredibly difficult.

However, even more pressing concerns are in the category of 'new' crimes, making it more difficult for law enforcement to be effective. On the buyer and vendor sides, law enforcement now has to worry about the increased availability of weapons for 'lone wolf' terrorists in regions such as Western Europe where stricter gun control regimes are in place.

New crimes are also present within technology, where law enforcement has to proportionally increase its talent base and understanding of how these technologies can be circumvented or tapped, how to combat new crimes such as mercenary hacking services, and how to co-ordinate technically intensive operations where data, and therefore local responsibility, run across dozens of national jurisdictions.

Among the few certainties in the chaotic, decentralised world of darknet markets is that growth on the part of buyers, vendors, markets, and the technology behind them will continue. Customers for illicit goods and services have so far been undeterred by law enforcement efforts, and the growth in the number of markets, listings, and associated services since the first major seizures behind Silk Road 1.0 reflects that.

Law enforcement response

As dozens of new markets have opened, further law enforcement efforts are likely to continue to drive markets to grow and specialise along regional and linguistic lines, offering diverse products from stolen credit cards to cannabis. According to Oerting, "Everything is for sale here – the rape of babies, guns, heroin, identity cards, passports, trojans, malware, social security numbers, credit card numbers – the list is endless. [There is] no decrease in the number of these services being established on the darknet – and more will most likely follow."

This trend in specialisation may also grow as a more discerning customer base looks for security and specific offerings, whether in bulk or in quality, among referral-only sites. This trend has already begun with regional markets such as RAMP or carding (credit card fraud) markets such as the Tor Carding Forum (TCF).

What is likely to remain stable in the chaotic underground is law enforcement policy. Despite the latest major seizures in November 2014 during Operation Onymous, law enforcement agencies still face clear obstacles in keeping up with technology. Moreover, law enforcement agencies are unlikely to adapt their policies to include harm reduction (deploying public health policies to lower risks of harm to, for example, drug users), as they have done on occasion in traditional anti-drug and anti-weapon programmes through the use of buybacks, needle exchange, or medical advice.

The upwards trending data for customer bases, vendor listings, and the proliferation of new markets might suggest that current law enforcement is ineffective in deterring or causing a dent in growth. However, this may also be another case of 'old world bureaucracy' being incompatible with new types of

technically driven crime. These new crimes offer law enforcement agencies the opportunity to bid for increased budgets for the hiring of new analysts, particularly those who specialise in computer security and engineering, but the approach does not yet encompass scope for harm reduction or other more progressive law enforcement strategies.

In the meantime, the anarchically free market on the darknet has sought its own solutions, with some major markets even hosting certified physicians to answer customer questions and dispense advice on the safe use of recreational drugs, or banning the sale of more dangerous products such as hard drugs and weapons. Others take a more commercial approach, with some vendors offering laboratory-tested narcotics to verify the "safety" and purity of products.

Overall, therefore – and given the slow evolution of current efforts of law enforcement to seek new policies that adapt better to online crime – future innovations are likely to come from non-governmental organisations and the markets or vendors themselves, with approaches including harm reduction and a degree of self-policing.

Outlook

Continuing current interdiction efforts may run into obstacles with regard to privacy rights and the underlying technologies. Law enforcement authorities themselves are conscious of the privacy issue. Oerting told *IHS Jane's*, "EC3 is a heavy supporter of privacy, both in the off- and online world. We will defend this legitimate right, which is... a cornerstone in all democracies. However, I am not convinced that privacy means anonymity... This is not about freedom of speech or protecting journalists or freedom fighters. This is [about] combating organised crime... conducted with the help of the anonymity the internet provides. And we will continue to do this in a targeted and proportionate way."

Since disrupting individual markets and identifying individuals who are major administrators or vendors is difficult, law enforcement and intelligence agencies are likely to seek to circumvent or undermine technologies such as Tor that protect them. Since their initial development, some have been quick to portray Tor or Bitcoin as government projects with backdoors that will allow law enforcement agencies to get ahead of digital crimes. Indeed, the latest major operations, including Onymous, have prompted activists from the privacy rights organisations such as the Electronic Frontier Foundation to raise concerns about the safety of the same networks that are used by political dissidents or others demanding technical protection for their free speech.

However, given that no shifts in current policy are likely, the technologies used today to power darknet markets are likely to be targeted by law enforcement, as well as the markets' customers. Some tools, such as PGP, are cryptographically assured and unlikely to be broken, but others such as Tor are demonstrably insecure if one agency or actor can control enough of the network to de-anonymise a majority of users.

'Continuing current interdiction efforts may run into obstacles with regard to privacy rights and the underlying technologies'

According to Welsh, "Law enforcement bodies are constantly seeking to exploit technology to disrupt criminal activity on the dark web, and identify and arrest offenders. This has created something akin to an arms race and that situation is likely to continue." However, he admitted that it was "an ongoing challenge for us to identify and exploit evolving technologies with at least the same speed and agility as criminal networks. Relationships with industry are particularly valuable in helping us to achieve this".

Despite the likelihood of these technologies being targeted and disrupted, and the abilities of cyber-criminals and others to develop them further, the platforms powering darknet markets are still unlikely to be dismantled. These underlying technologies have far greater economic potential in legitimate cases such as remittance markets (expatriates returning earnings to their home countries) or 'smart contracts' that can take advantage of the ease in global transfers and technical controls in payment processing.

Already, this legitimacy is being confirmed by the amount of venture capital accruing solely to Bitcoin and decentralised technology startups, which has exceeded USD200 million since 2012. Dedicated funds and major investors are involved. Although the darknet markets continue to grow in terms of the size of their customer base and the diversity of their products, they pale in comparison to the potential of the USD440-billion remittance market, where the same technology could be adopted with clear advantages.

Therefore, the future of illicit activity online remains possibly more anarchic, but with few certain outcomes for those involved. Law enforcement can count on increasing obstacles in combating illicit goods and services through interdiction online, but is likely to continue to follow the same policies because of the low political viability of harm reduction in many jurisdictions. Moreover, more nuanced strategies face a range of hiring and bureaucratic issues.

However, as interdiction efforts continue, markets will continue to proliferate in greater numbers following each takedown, with more specialised offerings underpinned by greater security and privacy technologies. The underlying technologies may be eventually circumvented by state signals intelligence agencies such as the US National Security Agency (NSA), due to possible overlap with high-priority targets such as terrorists and political actors, but these technologies are likely to continue to be developed because they also power a new range of legitimate uses, again backed by venture capital.

Consequently, the power of darknet markets may be better measured by the political and bureaucratic challenges they create, and the myriad legitimate opportunities they enable, than the relatively small part they play in the global drug or weapons trade. ■

This article was first published online at ***ihs.com/janes*** *on 30 December 2014.*

On the web

- Faceless crime – Criminal groups turn to cyber technology
- Social science helps to tackle organised crime

Author

Rodrigo Bijou is a cyber security expert in threat intelligence and privacy technology.

ihs.com/janes