As has happened with other complex IT and security technologies, enterprises will come to a point where they ask themselves whether security intelligence is core to their business or whether it's something that is easier, faster and less costly to implement and maintain if managed by outside experts. Security intelligence based on SIEM and big data implementations has the potential to be outsourced to service providers with the requisite experience, skills and implementation capabilities. Note that, for organisations with the most sensitive needs (many financial institutions, government agencies, etc), outsourcing to a service provider simply isn't a viable option. For these organisations, in-house implementations will continue to be the standard.

Explosion of devices

The Internet of Things trend will also change matters. Devices that collect all kinds of data are exploding in popularity, and it is only a matter of time before they start to become useful for security intelligence purposes. Indeed, power meters, cable modems, phones, medical devices, wireless access points, traffic density scanners and more will increasingly feed data into big data implementations. Interestingly, security-related big data implementations will result in new data sets that can be used for context aware pattern recognition and profiling. This information can then in turn be used to enhance current threat recognition, or to provide a logical check to prevent false positives based on less complete security profiles.

"Businesses of all sizes need adequate security intelligence mechanisms in place to monitor all activity across their networks, so that they can spot any suspicious activity and stop hackers in their tracks"

Data is becoming an increasingly valuable currency, and hackers are becoming more cunning in their attempts to steal it. For businesses, this has greatly increased the risk of reputational damage and called for a step change in current data security policies, particularly as consumers are rapidly losing patience with those who cannot safeguard their private information. As such, businesses of all sizes need adequate security intelligence mechanisms in place to monitor all activity across their networks, so that they can spot any suspicious activity and stop hackers in their tracks. However, as operational infrastructures become increasingly complex, security practises will need to evolve in tandem.

There remains the issue of how to fund the implementations and tools required to protect systems. Today's organisations are faced with the fundamental need to reprioritise their IT security spending to support these new tools. It's a hard decision for many who have spent decades keeping intruders at bay with the latest firewalls, network segmentation tools and endpoint defences – and these are now becoming less effective. It isn't that they should be eliminated, but they should no longer be the core focus of an organisation's security stance. A shift in spending priorities is needed.

About the author

Sol Cates is chief security officer for Vormetric and is tasked with ensuring the company's internal security profile remains robust, while maintaining a strong pulse on the technical and business decision- making process in today's IT/IS organisations. Cates partners with teams throughout the company and the industry to engage with both customers and partners. He is sought after to speak publicly to elevate industry understanding of data security best practices in today's complex cyber threat landscape. The technical depth and understanding of the information security space Cates has developed over the last 17 years is rooted in the intelligence community, financial services industry and other large enterprise organisations. He originally joined Vormetric in 2003, as a security engineer, and later became the senior director of field engineering and solutions architecture. Cates' career also includes technical sales, engineering and support leadership roles at Tripwire, Symantec, SignaCert and Spectra Physics, as well as consulting for many Fortune 500 companies and government agencies on cyber-security.

Should the dark net be taken out?

Cath Everett, freelance journalist

Cath Everett

Although the dark net is not necessarily something that many people outside the tight world of information security are hugely familiar with, its profile has been rising steadily over recent months. For example, it hit headlines around the world towards the end of last year, following the high-profile Operation Onymous, which was conducted by a mixture of US and EU international law enforcement agencies.[1]

Onymous targeted so-called 'dark markets', or online marketplaces operating on the dark net that sell illicit goods such as drugs, stolen credit card numbers and weapons. The aim was to raid and close down these illicit shopping sites, the most famous of which was Silk Road 2.0, which was only accessible via the Tor network – the original and most famous means of accessing the dark net.[2]

Tor, formerly known as The Onion Router, is a peer-to-peer network and browser employed by interested parties from the early 2000s to surf the Internet anonymously. It was originally developed by the US Navy in the mid-1990s in order to communicate with agents in the field without divulging their whereabouts, so as not to put them in danger.

But Tor, alongside other newer darknet file-sharing variants, such as JonDo, are now used by criminals, whistle-blowers and dissidents alike to enable them to communicate anonymously with trusted peers and avoid government snooping.[3]

"No-one really knows how big the dark net in its entirety is either because its services are by their very nature hidden"

As to how large the dark market black economy actually is in reality, though, no accurate statistics are currently available as no-one actually knows. In fact, no-one really knows how big the dark net in its entirety is either because its services are by their very nature hidden – although it is believed to be much smaller than the open Internet.

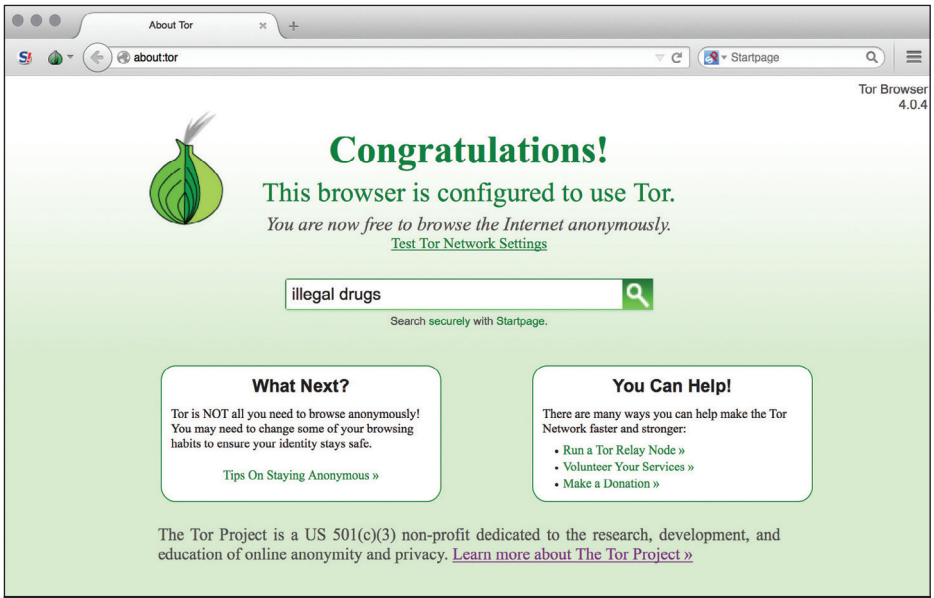
Hidden services

However, to give some inkling, members of the Tor project estimate that, on their network alone, there are between 1,000 and 1,200 hidden services and approximately three million users.

Operation Onymous, by way of contrast, led to the much-touted shutting down of around two-dozen hidden services and the arrest of some 17 marketplace vendors and administrators. Around $1m-worth of bitcoins, the standard currency for dark market transactions, as well as €180,000 in cash, drugs, gold and silver were also seized.

But it is worth noting that criminal activity in the dark net tends to be quite specific in nature, says Neil Hare-Brown, chief executive of information security consultancy Storm Guidance. For instance, most fraud and denial-of-service style attacks tend to be undertaken on the open Internet. "I don't know any denial of service attacks that have occurred through the dark web – it's so slow, it's like going back to the mid-1990s so it's just not performant enough," he explains.

On the other hand, Hare-Brown indicates that hackers undertaking targeted attacks would probably opt for the anonymity of the dark net. Criminals and terrorists also popularly employ it as a communications tool in order to help them plan activities. In addition, illegal shopping sites such as Evolution and Agora have now resulted in a situation where "most drugs are being bought and sold via the dark web – so many, in fact, it's amazing", he adds.



The Tor Browser Bundle allows anyone to use the web anonymously and easily.

Another recent moment in the spotlight for the dark web, meanwhile, was its name-checking by UK Prime Minister David Cameron last December when he unveiled the creation of a new government unit to target individuals using it to share child sex abuse images. The unit, which will be jointly run by British intelligence agency GCHQ and the National Crime Agency, which fights serious and organised crime in the UK, has yet to be assigned a name. But a key goal is to develop new high-tech ways of analysing vast quantities of child-related pornographic material on the dark net in order to better identify and arrest offenders.

Global network

Such activity would appear vital when, according to Tim Watson, director of the Cyber Security Centre at Warwick University, a huge 80% of all visits to dark net websites are to those hosting abusive images of children. As a result, focusing on paedophile activity as a starting point appears to make sense when trying to tackle dark net crime, with or without the inevitable elements of political expediency.

"A key goal is to develop new high-tech ways of analysing vast quantities of child-related pornographic material on the dark net in order to better identify and arrest offenders"

"If you look at high-tech crime units across the UK, traditionally about 70% of their activity is spent on paedophile stuff," Watson says. "There's lots of crime, but if it's a choice of going after people stealing credit card details or a gang abusing children who continue to be at risk, I think the public would probably support them in what they're doing."

In a move that should help such efforts further, some 30 countries around the world, including the US and UK, have likewise agreed to either set up their own national databases of child sex abuse content or provide links to Interpol's International Child Sexual Exploitation

Neil Hare-Brown, Storm Guidance: "Most drugs are being bought and sold via the dark web."

Database (ICSE DB).[4] ICSE makes it easier to share and remove these images once they emerge from the dark onto the open Internet, but the main objective in creating a global network is to make it easier to detect criminals and identify victims across international borders.

International cooperation

Nonetheless, the ongoing dearth of international legislation or even global harmonisation of national laws means that tackling crime on either the open Internet or the dark net remains a huge challenge.

Guillaume Lovet, threat intelligence lead at network security company Fortinet's FortiGuard Labs in Europe, the Middle East and Africa, explains that being able to arrest criminals, whether paedophiles or not, is only possible if they happen to be located in the same countries as their victims, which is rarely the case.

While the perpetrators are often based in Eastern Europe, South America or China, their victims are generally found in the West. "So Western Europe and the US can have all of the laws they want, but if the aim is to arrest someone in the East, they need cooperation there," he says.

The big question, though, is why countries elsewhere would bother to cooperate at all. As Lovet points out: "The victims are elsewhere and crime profits the local economy as the money generated in the West is taken back to the East, creating a chain of wealth creation."

As a result, most countries have no incentive to take action and, even if laws are passed to please the international community, they tend to be enforced only infrequently and under pressure. To make matters worse, the lack of bilateral agreements between individual countries outside of the European Union makes the bureaucracy involved in investigating international crime vast, which in turn makes such activity very expensive.

Storm Guidance's Hare-Brown explains: "This team from the UK will need to visit here and there and meet their dignitaries, officials, experts and the like. But it causes practical, logistical problems, which means you're very limited in the number of investigations that can be performed each year."

Nonetheless, he puts the relative success of Operation Onymous – despite widespread criticism in the information security community for overstating outcomes that later had to be revised – more down to "good, old-fashioned, standard police work" than any mind-blowing technical capabilities.

"Western Europe and the US can have all of the laws they want, but if the aim is to arrest someone in the East, they need cooperation there"

"Really it was about good investigation work, which involved following up leads and putting people under surveillance," Hare-Brown says. "I'd love to say it was about great high-tech skills and tools, but it was much more about the quality of the investigation."

National level

Even at the national level, however, the situation is far from straightforward. According to a recent UK Home Office report on cybercrime, not only is as little as 2-3% of such activity reported, but there is also no consistency between police forces on how they undertake investigations.

To compound the issue, law enforcement teams tend to be under-resourced, which means, in the words of Mike Gillespie, founder and managing director of information security consultancy Advent IM, it becomes "like chasing a spectre".

Tim Watson, Warwick University: "It's sometimes difficult for those parts of the police focusing on cybercrime to get the resources they need."

"It's like Del Boy in [the TV show] 'Only Fools and Horses' with his pop-up stalls. He sets them up, sells stuff from them for a while and then they pop up somewhere else – and it's the same with beta and mirror sites on the dark net," he says.

Shut down?

Despite the UK Government's rhetoric about its keenness to tackle the issue, it appears that at least some of the foot-dragging may have a political element.

"It's sometimes difficult for those parts of the police focusing on cybercrime to get the resources they need," explains Warwick University's Watson. "The government is waking up to the fact that we have a big hidden crime problem, but the question is does it really want to show crime figures shooting up, especially if there's not enough money to properly resource things?"

This ongoing situation has led to there being a significant skills gap within law enforcement agencies resulting in a lack of trained specialists – and even general awareness.

As John Walker, chief technology officer at Cytelligence, which offers organisations cyber-protection services, points out: "If you walked into the aver-

Mike Gillespie, Advent IM: Prosecuting cases is "like chasing a spectre".

age police station and said you'd been attacked by criminals in the dark net, they'd just stare at you."

All these difficulties notwithstanding, there appears to be little appetite to try and shut down the dark net completely – even if it were technically possible. Watson explains: "It's the equivalent of asking should we close down illegal activity in a city. You could shut the city, but the problem is that there's a lot of valid activity goes on there and where would everyone live?"

"If you walked into the average police station and said you'd been attacked by criminals in the dark net, they'd just stare at you"

For example, he pointed out, valid dark net activity is carried out by journalists, whistle blowers and dissidents fighting against totalitarian regimes. "So there's an argument to say that the benefits of having it in place outweigh the disadvantages, and I think a number of people would have difficulties if you said it was going to be completely closed down," Watson adds.

Advent IM's Gillespie agrees: "Just because you have nefarious elements doesn't make the technology evil. But the NSA has been quite vocal lately that if people use elements of the dark net, they will consider you a potential target."

A growing problem

The justification appears to be that, if someone choses to use Tor – "the whipping boy for the dark net" – they must have something to hide rather than simply preferring to have a bit of privacy. "But it's that kind of attitude that makes people wary of the whole security thing," Gillespie says.

"There's a fine line between national and international security and the protection of individuals and the masses," he continues. "We obviously want criminals to be caught, but you have to be careful. There's been a continual erosion of civil liberties in the UK over recent years and every time they've been handed over, we've been told it's in the interests of national security."

The proposed banning of encryption technology to enable UK intelligence services to access all digital communications is the latest case in point.

"The technology evolved to protect data in transit and at rest from criminals," says Gillespie. "So the danger is that we lose our protection against criminals so that the government can catch criminals. It doesn't make sense."

Nonetheless, there is concern that cybercrime on both the dark and open Internet is continuing to grow apace and is becoming ever more dangerous. For instance, one worrying trend is how progressively porous the boundaries between different types of cybercrime have become over the past 12 months.

In the past, crimes tended to be motivated by money, involved targeted attacks by state-sponsored hackers or were undertaken for ethical reasons by hactivists, or for fun. But the three are now starting to morph into each other, warns Fortinet's Lovet. For instance, in January last year, there were a series of targeted attacks on Target shops, followed by more in December on Home Depot. "So it seems that criminals motivated by money were starting to use the tactics of state-sponsored hackers and the like," he says.

Another concern is the progressive amount of consumer and corporate goods and services that come with IP addresses and network cards in order to connect them to the Internet.

John Walker, Cytelligence: "It's the equivalent of asking should we close down illegal activity in a city."

"Increasingly, everything is harmonising under one IP Internet-enabled system, which means that people can go wherever they want," Storm Guidance's Hare-Brown says. "Everything is becoming connected from smart fridges to corporate networks so hackers are now able to act with growing levels of impunity."

About the author

Cath Everett has been an editor and journalist for more than 20 years, specialising in information security, employment, skills and all things HR. She has worked in the online world since 1996, but also has extensive experience of print, having worked for publications ranging from The Guardian *to* The Manager. *She returned to the UK from South Africa at the end of 2014 where she wrote a lifestyle blog for International Business Times.*

References

1. 'Operation Onymous'. Wikipedia. Accessed Mar 2015. http://en.wikipedia.org/wiki/Operation_Onymous.
2. The Tor Project. Home page. Accessed Mar 2015. https://www.torproject.org.
3. 'JonDo – the IP changer'. Home page. Accessed Mar 2015. https://anonymous-proxy-servers.net/en/jondo.html.
4. 'Victim identification'. Interpol. Accessed Mar 2015. www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification.