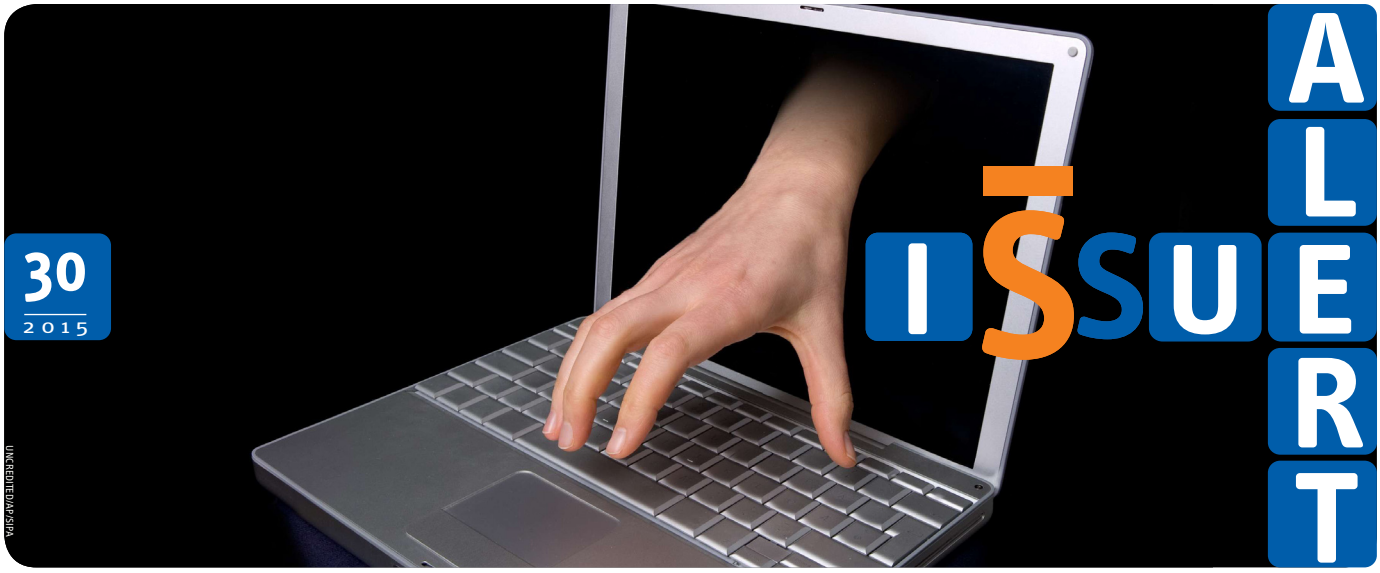

The dark side of the web: ISIL's one-stop shop?

by Beatrice Berton

In addition to its territorial expansion, the Islamic State of Iraq and the Levant (ISIL) has also embarked on a new campaign in the realm of cyber warfare. While Western law enforcement agencies are already tackling ISIL's propaganda, training programmes and recruitment drives on the mainstream web, the US Cyber Command has expressed its concerns over the growing penetration of terrorist organisations into the so-called *Dark Web*, the hidden underbelly of the online world's Deep Web.

The web we know and use every day, made up of websites accessible through conventional search engines such as *Google*, is referred to as the Surface Web. Few web users are aware that there is a Deep Web, a larger (about 500 times) section of the web consisting of websites, networks and online content which are not indexed by search engines. While much of this unindexed material is harmless, a smaller portion is intentionally hidden. It is within this unregulated environment that a variety of criminal organisations openly trade drugs, firearms, child pornography and other illicit materials.

An ideal ecosystem

ISIL's activities on the Surface Web are now being monitored closely, and the decision by a number of governments to take down or filter extremist content has forced the jihadists to look for new online safe havens. The Dark Web is a perfect alternative as it is inaccessible to most but navigable for the initiated few – and it is completely anonymous.

The most popular means of accessing and navigating the Dark Web is to use a Tor browser. Conceived by the US Navy as a means of protecting sensitive communications, the Tor browser allows users to hide their IP address and activity through a worldwide network of computers and different layers of encryption (like the layers of an onion), which guarantee their anonymity. Hidden services and marketplaces are listed on index pages such as the *Hidden Wiki* and are accessible only through Tor. *Silk Road*, a notorious online marketplace which sells drugs and weapons, was shut down by the FBI in 2013, but a variety of black markets such as *Agora*, *Evolution* and *AlphaBay* soon filled the void and welcomed many of the buyers and sellers previously associated with *Silk Road*.

The other side of Bitcoin

ISIL's adept use of social media makes the headlines, but the appeal of the Dark Web lies first and foremost in the anonymity of its services. *Sadaqa* (private donations) constitute one of ISIL's main sources of revenue, and its supporters around the world have allegedly used digital currencies such as Bitcoin to transfer money quickly to accounts held by ISIL militants while minimising the risk of detection. Cryptocurrency, the digital equivalent of cash, is often used for payments related to illegal trade, extortion or money laundering as it

particularly hard to trace. Dark Web marketplaces such as *Wall Street*, *Clone CC Crew* or *Atlantic Carding* might also be used as a source of additional funding because they specialise in selling stolen credit card details, hacked PayPal credentials and even stolen Uber accounts.

Weapons, tutorials and forums

While the EU boasts some of the toughest firearms regulations in the world, procuring guns within its borders is still possible, partly thanks to the Dark Web. *EuroGuns* is an online marketplace which deals in all kinds of weapons and sends them via regular mail. AK-47s – the type of assault rifle used by the Kouachi brothers in the Charlie Hebdo attacks – are sold for $550 each on *EuroArms*, one of the largest online black markets for purchasing weapons. In the spirit of Anwar al-Awlaki's brand of 'self-help' terrorism, several texts such as the *Terrorist's Handbook* and the *Explosives Guide* can also be purchased on *AlphaBay*.

As a result of strengthened border controls and legal constraints placed on individuals linked to ISIL, travelling to Syria and Iraq has become increasingly difficult for jihadist sympathisers. The Dark Web allows users to bypass some of these restrictions: *Fake Documents Service*, for instance, offers clients 'original high-quality fake passports, driver's licenses, ID cards, stamps and other products' for use in the UK, US, Australia and Belgium, among other countries.

Jihadist forums and chatrooms on the Surface Web were widely used by al-Qaeda in the mid-2000s. After raids by security services led to the arrest of several jihadist supporters, many extremist forums moved to the Dark Web, where private virtual spaces are encrypted and membership needs to be verified by administrators. Links and pathways to these closed-access spaces are then usually made available on the social media accounts of extremist groups. Occasionally, different terrorist groups compete for control of these forums: *Shumukh al-Islam*, for example, is a forum which oscillates between ISIL and al-Qaeda supporters. ISIL militants also profit from secure and private communication on the Dark Web: email services such as *Sigaint* and *TorBox* allow users to send and receive messages without revealing their location or identity.

Stopping the flow of resources...

ISIL's ability to generate funding online has allowed it to evolve from a regular terrorist group to a proto-state organisation. Michael S. Rogers, the head of US Cyber Command, recently stated that ISIL's activities on the Dark Web boost its capacity to sustain itself financially, as well as improve its operational effectiveness on the ground. Their recent military successes are likely to put more pressure on governments to grant law enforcement agencies access to encrypted communications by designing 'backdoors' in encryption software. Such proposals will, in turn, fuel already heated debates about citizens' privacy and civil liberties.

While law enforcement agencies have referred to the Dark Web as a 'gaping hole' and admitted that they often lack the tools and resources needed to protect citizens, online anonymity is widely regarded as a right. Moreover, privacy advocates argue that encryption is an essential tool for dissidents and activists living in countries ruled by oppressive regimes. While striking a balance between protecting civil liberties and maintaining security is not an easy task, the key challenge for governments is to prioritise tailored responses and strategies instead of plumping for widespread, indiscriminate monitoring strategies.

...by onymising the anonymous

The transnational nature of cyber jihadism means that any response requires a global approach. A case in point is the joint operation conducted by Europol, the FBI and the Department of Homeland Security in 2014, *Operation Onymous*, which led to the closure of over 400 black market websites and the arrest of 17 vendors and administrators. It has not yet been revealed whether law enforcement agencies have found a way of penetrating Tor's defences, but new efforts are underway to map out the hidden services available on the Dark Web.

The US Defense Advanced Research Projects Agency (DARPA) has developed new technology capable of finding content and analysing patterns of activity on the Dark Web. The *Memex* search engine, originally designed to counter human trafficking rings, will be instrumental in identifying ISIL's cyber activities and limiting their access to online resources. With ISIL actively looking for hackers and computer scientists to bolster its ranks, law enforcement authorities need to continue investing in the training of cybersecurity experts and the strengthening of forensic capacities. But most of all, they need to make better use of the existing frameworks for international cooperation.

Beatrice Berton is a Junior Analyst at the EUISS.

 | QN-AL-15-030-2A-N | ISBN 978-92-9198-325-4 | ISSN 2315-1129 | DOI 10.2815/454889