Going Darker?

THE CHALLENGE OF DARK NET TERRORISM

PROF. GABRIEL WEIMANN
Dept. of Communication, University of Haifa, Israel
Public Policy Fellow at the Woodrow Wilson Center, Washington, DC, USA

Wilson Center

INTRODUCTION

When most people think of the Dark Net, they think of crime, fraud, illegal online activities and terrorism. But what really is the Dark Net? Why is it appealing to internet-savvy terrorists? How can we counter this new age of terrorism? Perhaps most crucially, is the Dark Net all Dark?

Think of the Internet as a huge iceberg. The tip of the iceberg, which most people can see, is the Surface Web that has been crawled and indexed, and is thus searchable by standard search engines such as Google or Bing via a regular web browser. But the majority of the Internet lies below the metaphorical waterline, unsearchable and inaccessible to the general public. These hidden parts of the internet are known as the Deep Web. The Deep Web is approximately 400-500 times more massive than the Surface Web.[1]

The deepest layers of the Deep Web, a segment known as the Dark Net, contains content that has been intentionally concealed including illegal and anti-social information. The Dark Net can be defined as the portion of the Deep Web that can only be accessed through specialized browsers (like the Tor browser). A recent study found that 57% of the Dark Net is occupied by illegal content like pornography, illicit finances, drug hubs, weapons trafficking, counterfeit currency, terrorist communication, and much more.[2]

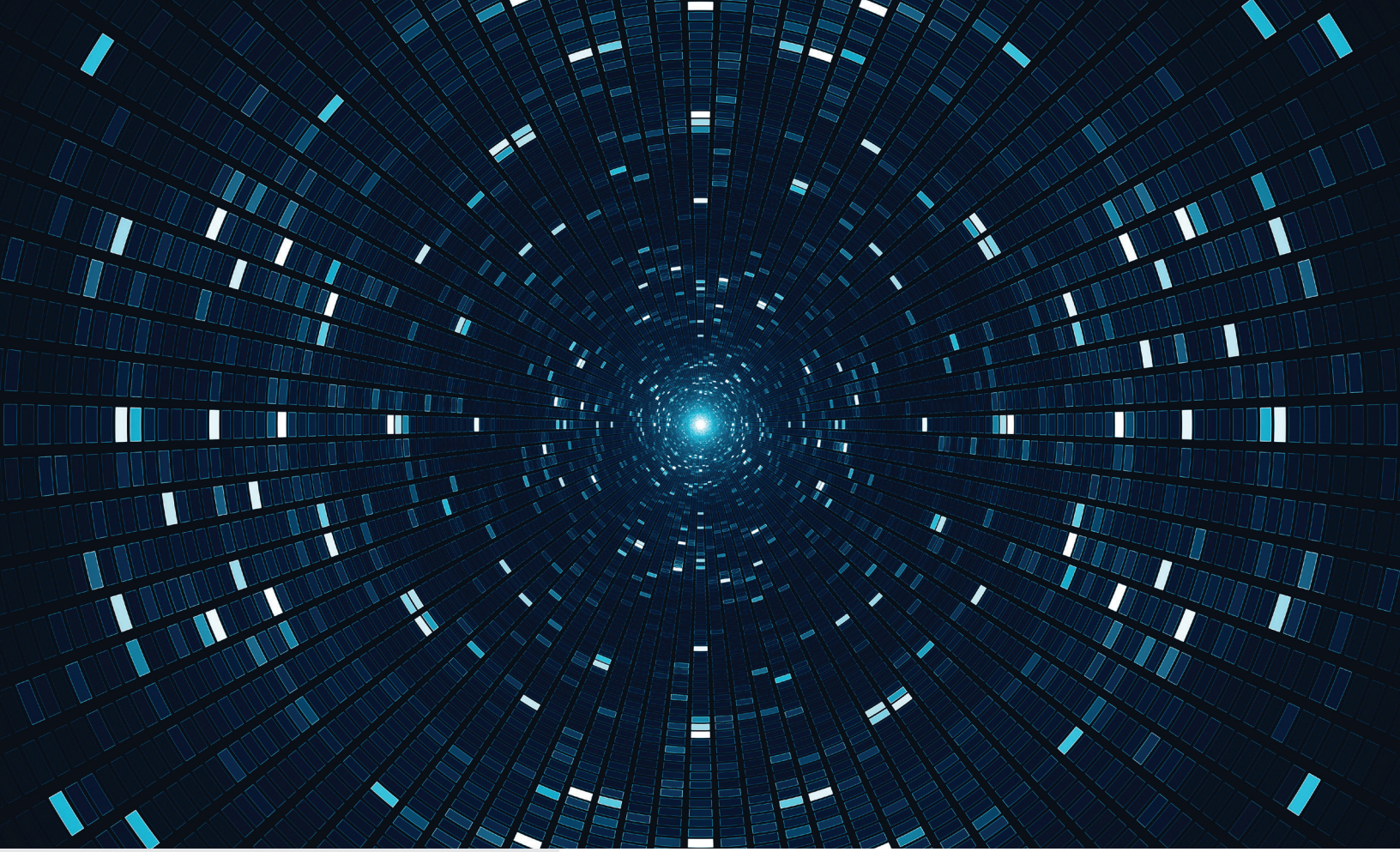
Probably the most notorious example of these Dark Net activities can be seen in The Silk Road. In October 2013, the FBI shut down the first version of this drug market and arrested its owner Ross William Ulbricht. Since the arrest of Ulbricht in 2013, dozens of Silk Road replacements have sprung up in Medusa-like fashion as hidden services deployed on the Dark Net. The Dark Net has been associated with the infamous WikiLeaks, as well as Bitcoin, said to be the currency of the Dark Net. Of course, dissident political groups, civil rights activists and investigative journalists in oppressive countries have also been known to use the Dark Net to communicate and organize clandestinely.

Terrorists, too, have revealed the advantages of the Dark Net and started using its secretive platforms. Although it has long been assumed that terrorist attacks are coordinated in a secret network, solid evidence of terrorist use of Dark Net platforms has only been attained in 2013. In August 2013, the U.S. National Security Agency (NSA) intercepted encrypted communications between al-Qaeda leader Ayman Al-Zawahiri and Nasir Al-Wuhaysi, the head of Yemen-based al-Qaeda in the Arabian Peninsula. The Institute for National Security Studies revealed that, for about a decade, the communication between leaders of the worldwide al-Qaeda network was at least partially leveraged on the Dark Net.[3]

Wilson Center

WOODROW WILSON INTERNATIONAL CENTER FOR SCHOLARS

The Woodrow Wilson International Center for Scholars, established by Congress in 1968 and headquartered in Washington, D.C., is a living national memorial to President Wilson. The Center's mission is to commemorate the ideals and concerns of Woodrow Wilson by providing a link between the worlds of ideas and policy, while fostering research, study, discussion, and collaboration among a broad spectrum of individuals concerned with policy and scholarship in national and international affairs. Supported by public and private funds, the Center is a nonpartisan institution engaged in the study of national and world affairs. It establishes and maintains a neutral forum for free, open, and informed dialogue. Conclusions or opinions expressed in Center publications and programs are those of the authors and speakers and do not necessarily reflect the views of the Center staff, fellows, trustees, advisory groups, or any individuals or organizations that provide financial support to the Center.



ACCESSING THE **DARK NET**

If so motivated, any internet user can visit the Dark Net. Individuals can access the Dark Net by using special software such as Tor (short for The Onion Router) or I2P (Invisible internet Project). Tor was initially created by the U.S. Naval Research Laboratory as a tool for anonymously communicating online. It relies on a network of volunteer computers to route users' Web traffic through a series of other users' computers so that the traffic cannot be traced to the original user. Some developers have created tools—such as Tor2- web—that allow individuals to access Tor-hosted content without downloading and installing the Tor software.

However, tracking visitors - and content producers – is trickier than on the mainstream internet. In most cases, a visitor to a .onion site, more commonly known as a Dark Net site, will not know the identity of the host, nor will the host know the identity of the visitor. This is very different from the mainstream internet, where sites are often associated with a company or location and visitors are often identified and monitored through sundry tracking technologies such as cookies, account registrations, Flash cookies, IP addresses, and geolocation. In the mainstream internet, there is a clear trail – not so on the Dark Net, where anonymity reigns.

Not all Dark Net sites use Tor, but the principle remains the same. The visitor has to use the same encryption tool as the site and—crucially—know where to find the site, in order to type in the Uniform Resource Locator (URL) and visit. Once on the Dark Net, users often navigate it through directories such as the "Hidden Wiki," which organizes sites by category, similar to Wikipedia. In the Dark Net, individuals may communicate through means such as secure e-mail, Web chats, or personal messaging hosted on Tor.[4]

TERRORIST INTEREST IN THE DARK NET

Terrorists have been active on various online platforms since the late 1990s.[5] The Surface Web, however, was revealed to be too risky for anonymity-seeking terrorists: they could be monitored, traced and found. Many of the terrorist websites and social media on the Surface Web are monitored by counter-terrorism agencies and are often shut down or hacked. In contrast, on the Dark Net, decentralized and anonymous networks aid in evading arrest and the closure of these terrorist platforms. "ISIS'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," Beatrice Berton of the European Union Institute for Security Studies wrote in her report on ISIS's use of the Dark Net.[6]

Following the attacks in Paris in November 2015, ISIS has turned to the Dark Net to spread news and propaganda in an apparent attempt to protect the identities of the group's supporters and safeguard its content from hacktivists. The move comes after hundreds of websites associated with ISIS were taken down as part of the Operation Paris (OpParis) campaign launched by the amorphous hacker collective Anonymous. ISIS's media outlet, Al-Hayat Media Center, posted a link and explanations on how to get to their new Dark Net site on a forum associated with ISIS.

In April 2018 a report, entitled "Terror in the Dark", summarizes the findings of a study conducted by the Henry Jackson Society, revealing the growing use of the Dark Net by terrorist groups.[7] The findings illustrate how terrorists and extremists are creating growing numbers of safe havens on the Dark Net to plot future attacks, raise funds and recruit new followers. This report highlights the following uses of the Dark Net for terrorist purposes:

1. Terrorists use the Dark Net to hide: The monitoring of the surface web by social media companies and security officials has resulted in a faster rate of removal of extremist content from social media platforms. Correlated with this is an increased use by terrorist networks of the Dark Net for communication, radicalization and planning attacks.
2. Terrorists use the Dark Net for recruitment: While initial contact can be made on surface web platforms, further instructions are often given on end-to-end encryption apps such as Telegram on how to access jihadist websites on the Dark Net.
3. Terrorists use the Dark Net as a reservoir of propaganda: The removal of extremist and terrorist content from the surface web increases the risk that material of terrorist organizations may be lost. Much of this material later resurfaces on the Dark Net.
4. Terrorists use virtual currencies to evade detection and to fundraise: Terrorists, like criminals, use cryptocurrency because it provides the same form of anonymity in the financial setting as encryption does for communication systems.

In the last two years, I have monitored the emergence of terrorists on the Dark Net. My early findings revealed indications of the growing terrorist interest in the dark online platforms.[8] However, over time, monitoring of online terrorism added new indications, new findings and new trends of terrorist presence in the Dark Net. Let me review some of these findings and trends.

WHAT ARE **TERRORISTS DOING** ON THE DARK WEB?

A simple description of what terrorists do on the Dark Net would be, "more of the same but more secretly." However, that is only partially true. Terrorists are using the Dark Net as they have been using the Surface Web for several decades, but there are also new opportunities offered now to cyber-savvy operatives. Terrorists have used the "open" internet to provide information to fellow terrorists, to recruit and radicalize, to spread propaganda, to raise funds, and to coordinate actions and attacks. Some of this activity, however, has now shifted to deeper layers of the internet. Terrorist propaganda material, for example, is now stowed in the Dark Net.

Terrorists are now using the Dark Net to communicate in safer ways than ever before. In March 2016, the French Interior Minister, Bernard Cazeneuve argued that the Dark Net is extensively being used by the terrorists. In a meeting of the National Assembly, he said that those who have been responsible for the recent terrorist strikes in Europe have been making use of the deep web and communicating through encrypted messages. Following the November 2015 attacks in Paris, ISIS has turned to the Dark Net to spread news and propaganda in an apparent attempt to protect the identities of the group's supporters and safeguard its content from hacktivists. The move comes after hundreds of websites associated with ISIS were taken down as part of the Operation Paris (OpParis) campaign launched by the amorphous hacker collective Anonymous. ISIS's media outlet, Al-Hayat Media Center, posted links and explanations on how to get to their new Dark Net site on a forum associated with ISIS. The site contains an archive of ISIS propaganda materials, including its documentary-style film, The Flames of War.

Recently, ISIS and other jihadist groups have used new online applications that allow users to broadcast their messages to an unlimited number of members via encrypted mobile phone apps such as Telegram. Telegram is an application for sending text and multimedia messages on Android, iOS, and Windows devices. It was founded by Russian entrepreneur Pavel Durov in 2013. One of the key features of Telegram is end-to-end encryption. This means even the creators of the app do not know the users' identity, making it very appealing to criminals and terrorists. The company behind Telegram is so confident of its security that it twice offered a $300,000 reward to the first person who could crack its encryption. Thus, Telegram's features and especially the deeper and more secretive forms of communication it offers, relate it to Dark Net users and contents. The ISIS announcement on its new Dark Net website was also distributed on Telegram.

Telegram has seen major success, both among ordinary users as well as terrorists. However, it was not until its launch of "channels" in September 2015 that the Terrorism Research & Analysis Consortium (TRAC) began to witness a massive migration from other social media sites, most notably Twitter, to Telegram.[9] On September 26, 2015, just four days after Telegram rolled out channels, ISIS media operatives on Twitter started advertising the group's own channel dubbed Nashir, which translates to "Distributor" in English. A recent ICT special report on Telegram revealed, "Since September 2015, we have witnessed a significant increase in the use of the Telegram software (software for sending encrypted instant messages) by the Islamic State and al-Qaeda. In March 2016 alone, 700 new channels identified with the Islamic State were opened".[10] When asked about it, Telegram's CEO Pavel Durov conceded that ISIS indeed uses Telegram to ensure the security of its communications, but added: "I think that privacy, ultimately, and our right for privacy is more important than our fear of bad things happening, like terrorism." [11]

While many of the channels have Islamic State affiliations, there is an increasing number of channels from other major players in the global jihadi world: these include al-Qaeda in the Arabian Peninsula (AQAP), Ansar al-Sharia in Libya (ASL) and Jabhat al-Nusra (JN) and Jaysh al-Islam, both in Syria. Al-Qaeda's branch (AQAP) launched its own Telegram channel on 25 September 2015 and the Libyan Ansar al-Shari'ah group created its channel the following day. According to a TRAC report, membership growth for each discrete channel is staggering. Within a week's time, one single Islamic State channel went from 5,000 members to well over 10,000.[12] Thus, as an ICT report concludes, "terrorist organizations continue to distribute defensive guidelines and instructions, and to expand their activities on the Darknet where they claim to be better able to protect the traffic and anonymity of the organizations themselves, as well as their supporters, from the tracking software of intelligence agencies and activists who operate against terrorist organization on the internet".[13] But communication is not the only exchange that we have to worry about on the Dark Net. The new alarming development is the use of virtual currencies by terrorists.

DARK NET **CURRENCIES**

The Dark Net is also used by terrorists as well as criminals for clandestine transfer of funds, using virtual currencies. This recent trend is one of the most alarming combinations of terrorism and the Dark Net capabilities. Cryptocurrency, the digital equivalent of cash, is often used for payments related to illegal trade, extortion or money laundering by criminals. Terrorists too can use the Dark Net for fundraising, money transfers and illegal purchase of explosives and weapons, using virtual currencies like Bitcoin and other crypto-currencies. In 2014, an article titled, "Bitcoin wa Sadaqat al-Jihad" which translates to "Bitcoin and the Charity of Violent Physical Struggle," was published online.[14] The article promotes the use of Bitcoin virtual currencies as a means of facilitating economic support for jihadists and circumventing the Western banking system, which limits donations for jihad through restrictions on the financial system. By using this digital currency, argues the Jihadi author under the pseudonym of Amreeki Witness, "one can prevent his 'brothers' who live outside the borders of the Caliphate from having to pay taxes to the infidels while simultaneously financing the mujahideen without exposing them to any legal risk."

In January 2015, the Singapore-based cyber intelligence company S2T uncovered concrete evidence that a terror cell, purporting to be related to Islamic State and operating in the Americas, is soliciting Bitcoin as part of its fundraising efforts.[15] The online message from the group's fundraiser, a man later identified only as Abu-Mustafa, declared: "One cannot send a bank transfer to a mujahid [engaged in Jihad] or suspected mujahid without the kafir [infidel] governments ruling today immediately being aware …A proposed solution to this is something known as Bitcoin …To set up a totally anonymous donation system that could send millions of dollars' worth of Bitcoin instantly…right to the pockets of the mujahideen, very little would be done [against it]".[16] Another example comes from Indonesia where a Jihadist group collected donations, both from national and international donors, through Bitcoins on the Dark Net. Furthermore, after acquiring a stolen identity from the Dark Net, the group hacked a Forex trading website to use the points of the member. From these series of cybercrimes, the terrorist group collected USD 600,000.[17]

In June 2015, the European Union published a report according to which supporters of terrorism allegedly transfer private donations using Bitcoin. The report stated that, according to the head of U.S. Cyber Command, activities by the Islamic State on the Dark Net will expand the organization's ability to strengthen itself economically and to improve the efficiency of its physical operations.[18] The ICT report (2018) entitled "Jihadists' Use of Virtual Currency" lists several cases of terrorist groups using virtual currencies for fundraising and purchase of weapons.[19] Following the terrorist attack at the Bataclan theatre in Paris, November 13, 2015, which claimed the lives of 89 people, the hacker group 'Ghost Security Group' tracked the digital footprints of the perpetrators of the attack. The group successfully uncovered a number of Bitcoin addresses that seemingly belonged to members of the organization.[20] Three million dollars were found in one account.

The Telegram account, "Technical Support of Afaq Electronic Foundation", a media group associated with ISIS, posted an answer to another user's question concerning whether Bitcoin purchases are secure.[21] After a short explanation about what Bitcoin currency is, the account offered a better alternative to secure online purchasing via Zcash, another virtual currency (Telegram, October 18, 2017).

In December 2017, a Federal District Court in New York indicted Zoobia Shahnaz of Long Island for bank fraud and money laundering that allegedly supported terrorism. Shanhnaz was accused of having defrauded several financial entities, stealing and laundering over $85,000 of illegal returns using Bitcoin digital currency and other digital currencies. Moreover, the funds were transferred out of the country in order to support ISIS.

In November 2017, the Akhbar al-Muslimin website, which publishes news from the Islamic State, launched an online fundraising campaign. The posting included a call for donations using Bitcoin. A study examining this campaign found that clicking on the link led to a dedicated donations page on a Bitcoin trading site called CoinGate.[22] Under every article on this new site there is a link reading, "Click here to donate Bitcoins to the [Akhbar al-Muslimin] website – do not donate from *zakat* funds" (i.e., funds earmarked for charity, one of the Five Pillars of Islam).

In summary, sporadic evidence of terrorists' use of digital currency have been documented since 2012 and there is no doubt that in recent months this trend has been growing and taking shape and now holds a prominent presence online. The examples presented above and other studies reveal that that the use of virtual currencies is prevalent at various levels, including the organization itself (the Islamic State), support groups and individuals.

COUNTERING **DARK NET** TERRORISM

Although the internet has been available to the public since the 1990s, the Dark Net has only emerged in recent years. The growing sophistication of terrorists' use of the Dark Net presents a tough challenge for governments, counter-terrorism agencies, and security services. When IBM's security division published its security threats report for 2015, it highlighted the threat of cyberattacks coming from the Dark Net, using Tor networks.

There is clearly an urgent need to develop new methods and measures for tracking and analyzing terrorist use of the Dark Net. Thus, for example, the Defense Advanced Research Projects Agency (DARPA) believes the answer can be found in MEMEX, a software that allows for better cataloguing of Deep Web sites. MEMEX was originally developed for monitoring human trafficking on the Deep Web, but the same principles can be applied to almost any illicit Deep Web activity.

In 2014, an investigation of the source code in one National Security Agency (NSA) program called XKeyscore (revealed by the Edward Snowden leaks), showed that any user simply attempting to download Tor was automatically fingerprinted, essentially enabling the NSA to know the identity of millions of Tor users. According to a report from the German media outlet Tagesschau, there are nine servers running Tor, including one at the Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory. All are under constant NSA surveillance. The NSA source code also revealed some of the behavior that users exhibit can immediately be tagged or "fingerprinted" for so-called deep packet inspection, an investigation into the content of data packages sent across the internet, such as e-mails, Web searches and browsing history. [23]

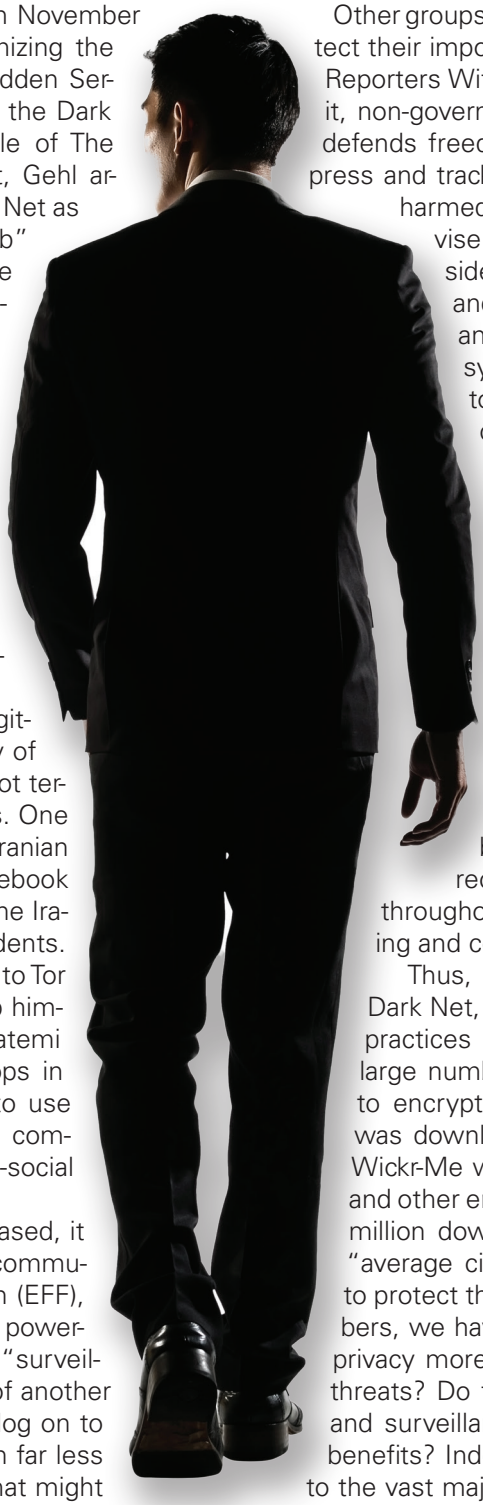
Tor, the most frequently used browser for Dark Net users is also targeted: Tor is a high-priority target for the National Security Agency. The work of attacking Tor is executed by the NSA's application vulnerabilities branch, which is part of the systems intelligence directorate, or SID. According to the whistleblower Edward Snowden, one successful technique the NSA has developed involves exploiting the Tor browser bundle, a collection of programs designed to make it easy for people to install and use the software. The first step of this process is finding Tor users. To accomplish this, the NSA relies on its vast capability to monitor large parts of the internet. This is done via the agency's partnership with U.S. telecommunication firms.

In February 2015, a special report entitled "The Impact of the Dark Web on Internet Governance and Cyber Security" presented several suggestions regarding the Dark Net.[24] The report states that "in order to formulate comprehensive strategies and policies for governing the internet, it is important to consider insights on its farthest reaches—the Deep Web and, more importantly, the Dark Web." It also notes "While the Dark Web may lack the broad appeal that is available on the Surface Web, the hidden ecosystem is conducive for propaganda, recruitment, financing and planning, which relates to our original understanding of the Dark Web as an unregulated space."

Despite the clear uses of the Dark Net for nefarious purposes, a question remains: is the Dark Net all dark or is the war against these illicit uses of this platform harming benign actors too?

WEB SIDE STORY: DARK NET IS NOT ALL DARK

Despite the common perception that the Dark Net is equivalent to the Evil Net, it is necessary to remember that the Dark Net also serves journalists, civil rights advocates, and democracy activists—all of whom may be under threat of censorship or imprisonment. In November 2017 Robert Gehl wrote about "Legitimizing the Dark Web: The New York Times's Tor Hidden Service", highlighting the important roles of the Dark Net for journalists.[25] Using the example of The New York Times's use of the Dark Net, Gehl argues that the common definition of Dark Net as "anything bad that happens on the Web" is misguided. Not all Dark Net users are bad, considering the fact that this platform may be the only available and safe venue for "good actors" as activists and dissidents, journalists, whistleblowers and citizen debating controversial issues without fear of being monitored. As Gehl argues, "Ultimately, the New York Times's presence on the Tor network delegitimizes the argument that the Dark Web is pure evil".[26] Journalists are certainly enjoying the anonymity provided by the Dark Net when communicating with their sources.



The utility of the Dark Net for more legitimate purposes goes back to the history of the network. Tor's early adopters were not terrorists or criminals, they were dissidents. One of them was Nima Fatemi, a 27-year-old Iranian who had been uploading photos on Facebook and Twitter to spread breaking news of the Iranian government's crackdown on dissidents. Under increased scrutiny, he had turned to Tor to continue working secretly and to help himself and his fellow activists stay safe. Fatemi was conducting private online workshops in Iran, teaching friends and family how to use the software and thus hide their online communication.[27] Use of the Dark Net by pro-social activist groups is still critical today.

Since the Tor software has been released, it has spread virally into several activist communities. The Electronic Frontier Foundation (EFF), the digital-rights group promoted Tor as a powerful pro-democracy tool, referring to it as "surveillance resistance." By using Tor in place of another browser, protesters and journalists can log on to Twitter or surf dissident chat rooms with far less risk of being tracked by a government that might imprison them or worse. During the Arab Spring, Tor helped facilitate protests throughout the Middle East. Nasser Weddady, a 39-year-old Mauritanian-American activist, was living in the States and began promoting the underground browser — becoming one of the most influential social-media dissidents during the uprising. "There would be no access to Twitter or Facebook in some of these places if you didn't have Tor," he says. "All of the sudden, you had all these dissidents exploding under their noses, and then down the road you had a revolution."[28]

Other groups that use Tor and the Dark Net tools to protect their important activities include organizations like Reporters Without Borders, an international non-profit, non-governmental organization that promotes and defends freedom of information and freedom of the press and tracks prisoners of conscience and jailed or harmed journalists all over the world. They advise journalists, sources, bloggers, and dissidents to use Tor to ensure their privacy and safety. Tor is also part of SecureDrop, an open-source whistleblower submission system that media organizations can use to securely accept documents from and communicate with anonymous sources. Many news organizations use SecureDrop, including the Associated Press, The Washington Post, The New York Times, The CBC, ProPublica, Dagbladet, and more. Human rights groups and activists also use Tor to anonymously report abuses from danger zones. For example, Human Rights Watch recommends the use of Tor in their report, "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." They cover Tor in the section on how to breach the "Great Firewall of China," and recommend that human rights workers throughout the globe use Tor for "secure browsing and communications."[29]

Thus, before considering actions against the Dark Net, these pro-social, non-terrorist users and practices need to be considered. For example, a large number of mobile phone users have turned to encrypted messaging apps. In 2016, Telegram was downloaded 49.28 million times, followed by Wickr-Me with 3.8 million, Signal with 3.62 million, and other encrypted messaging combined with 0.35 million downloads. This means a large number of "average citizens" are using the Dark Net, mainly to protect their privacy. When we look at these numbers, we have to ask ourselves, if our citizens value privacy more than they value security from terrorist threats? Do the costs of losing privacy, free speech and surveillance-free communications outweigh the benefits? Indeed, the number of terrorists compared to the vast majority of Telegram, Tor and other encrypted apps users who are benign and have no intention to commit an act of terror is very low. The alarming infiltration of internet-savvy terrorists to the "virtual caves" of the Dark Net should trigger an international search for a solution to combat illegal and nefarious activities, but one that should not impair legitimate, lawful freedom of expression.

ENDNOTES

1 See the Wilson Center report "The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box", at: https://www.wilsoncenter.org/sites/default/files/deep_web_report_october_2015.pdf

2 Moore, Daniel. & Rid, Thomas. 2016. "Cryptopolitik and the Darknet", Survival, 58:1, 7-38. Accessed April 30, 2016.URL: http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085

3 The Institute for National Security Studies (INSS), 2013. "Backdoor Plots: The Darknet as a Field for Terrorism", September 10, 2013.UTL: http://www.inss.org.il/index.aspx?id=4538&articleid=5574

4 Finklea, Kristin, Dark Web, special report for Congressional Research Service, 2015. Available at http://www.fas.org/sgp/crs/misc/R44101.pdf

5 Weimann, Gabriel. 2006. Terror on the Internet. Washington, DC: United States Institute of Peace; Weimann, G. 2015. Terrorism in Cyberspace: The Next Generation. New York: Columbia University Press.

6 Berton, Beatrice, 2015. "The dark side of the web: ISIL's one-stop shop?". Report of the European Union Institute for Security Studies, June 2015. Accessed March 1, 2016. URL:http://www.iss.europa.eu/uploads/media/Alert_30_The_Dark_Web.pdf

7 Malik, N. 2018. "Terror in the Dark", a report by the the Henry Jackson Society, London. At: http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

8 Weimann, Gabriel, 2016a. "Going Dark: Terrorism on the Dark Web", Studies in Conflict & Terrorism 39, 195-206. URL: http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546; Weimann, G. 2016b. "Going Dark: Terrorism on the Dark Web", Studies in Conflict & Terrorism 39, 195-206.

9 TRAC. 2015. "Massive Migration to Telegram, the new Jihadist Destination", TRAC Insight, November 4, 2015. URL: http://www.trackingterrorism.org/chatter/trac-insight-massive-migration-telegram-new-jihadist-destination

10 Cited in "Supporter of Extremist Group ISIS Explains How Bitcoin Could Be Used To Fund Jihad", Business Insider, July 8, 2014. http://www.businessinsider.com/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7

11 Cited in the Washington Post, November 19, 2015.URL: https://www.washingtonpost.com/news/morning-mix/wp/2015/11/19/founder-of-app-used-by-isis-once-said-we-shouldnt-feel-guilty-on-wednesday-he-banned-their-accounts/

12 TRAC. 2015. "Massive Migration to Telegram, the new Jihadist Destination", op. cit.

13 International Institute for Counter Terrorism (ICT), Cyber Terrorism Activities Report no. 19, December 2016, p. 10.

14 The document is online; URL: https://alkhilafaharidat.files.wordpress.com/2014/07/btcedit-21.pdf

15 "U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests", Haaretz, January 29, 2015. http://www.haaretz.com/middle-east-news/.premium-1.639542

16 Cited in "Supporter of Extremist Group ISIS Explains How Bitcoin Could Be Used To Fund Jihad", Business Insider, July 8, 2014. http://www.businessinsider.com/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7

17 Wimmer and Nastiti, 2015, op. cit.

18 Berton, 2015, op. cit.

19 International Institute for Counter Terrorism (ICT), 2018. Jihadists' Use of Virtual Currency, at: https://www.ict.org.il/images/Jihadists%20Use%20of%20Virtual%20Currency.pd

20 https://www.newsbtc.com/2015/11/14/isil-militants-linked-to-france-terrorist-attacks-had-a-bitcoin-address-with-3-million-dollars/

21 Ibid, p. 5

22 "Drive for Bitcoin donations on an ISIS-affiliated website", at: http://www.terrorism-info.org.il/en/drive-bitcoin-donations-isis-affiliated-website/

23 Tucker, Patrick, "If You Do This, the NSA Will Spy on You," Defense One, 7 July 2014. Available at http://www.defenseone.com/technology/2014/07/if-you-do-nsa-will-spy-you/88054/ (accessed 10 October 2015).

24 Chertoff, Michael and Simon, Tobby. 2015. "The Impact of the Dark Web on Internet Governance and Cyber Security". https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf

25 Gehl, Robert, 2017. "Legitimizing the Dark Web: The New York Times's Tor Hidden Service", http://culturedigitally.org/2017/11/legitimizing-the-dark-web-the-new-york-timess-tor-hidden-service/

26 Ibid., p. 3.

27 Kushner, David, 2015. The Darknet: Is the government Destroying the Wild West of the Internet"?, Rolling Stone, October 22, 2015, at https://www.rollingstone.com/politics/news/the-battle-for-the-dark-net-20151022

28 Ibid

29 https://www.hrw.org/reports/2006/china0806/

ABOUT THE AUTHOR

Gabriel Weimann, Public Policy Fellow at the Woodrow Wilson Center, is a Full Professor of Communication at the Department of Communication at Haifa University, Israel. His research interests include the study of media effects, political campaigns, persuasion and influence, modern terrorism and the media. He published 9 books and more than 180 academic publications in scientific journals. He received numerous grants and awards from international foundations and was a Visiting Professor at various universities including University of Pennsylvania, Stanford University, Hofstra University, Lehigh University (USA), University of Mainz (Germany), Carleton University (Canada), the American University (Washington, DC), NYU branch in Shanghai (China) and the National University of Singapore. His books include *Terror on the Internet* (2006) and *Terrorism in Cyberspace: The Next Generation* (2015).

THIS PROJECT WAS SUPPORTED BY A GRANT FROM THE CENTER OF CYBER, LAW AND POLICY (CCLP) AT THE UNIVERSITY OF HAIFA, ISRAEL.

Digital Futures Program

Wilson Center

@WilsonCenterDFP

Wilson Center

@WilsonCenter
facebook.com/WoodrowWilsonCenter
www.wilsoncenter.org

Woodrow Wilson International Center For Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027