The Perpetuation of Criminal Activity: The Formalization of the Dark Web as a Business Medium
Calvin Nobles, PhD
Cybersecurity Policy Fellow, New America Think Tank

“There’s a compounding and unraveling chaos that is perpetually in motion in the Dark Web's toxic underbelly.”
— James Scott, Senior Fellow, Institute for Critical Infrastructure Technology

The Internet is one of the most significant interventions in the world. Most users do not understand the difference between the Internet, the deep web, and the dark web (Chertoff & Simon, 2015; Chertoff, 2017). The Internet is an extensive network of networks consisting of all the systems and devices enabling global communication (Chertoff, 2017). Chertoff and Simon (2015) defined the world wide web as the way end-users access information over the Internet using a hypertext transfer protocol to transmit data. The Internet is divided into two subcategories: (a) surface web and (b) deep web (Chertoff, 2017). The surface web is a portion of the Internet that people use to access search engines such as Google, Yahoo, and Bing to access indexed websites (Vogt, 2017). Researchers classify the deep web as part of the Internet that is hidden and not indexed for routine use by end-users, which is 4000 to 5000 times larger than the surface web (Finklea, 2015; Chertoff, 2017). For users to access websites on the deep web requires one to know the exact uniform resource locator, which is commonly known as URL (Vogt, 2017). The deep web traffic is estimated at 90% of all Internet traffic given that sites like Facebook, Google, LinkedIn, and Twitter are application program interfaces that provide access to the sites in the deep web (Chertoff, 2017).

Within the channels of the deep web is an area known as the dark web or darknet, which Vogt (2017) describes as inaccessible and purposely not indexed to avoid accessibility from conventional search engines. The dark web or darknet of the deep web that is difficult to access and accounts for 0.01% of websites on the Internet in which researchers estimate that there are 45,000 websites on the darknet compared to hundreds of millions on the Internet (Chertoff, 2017). The secrecy of the dark web proliferates criminal activity such as (a) child pornography, (b) drug trading, (c) selling of compromised and stolen data, (d) money laundering, and a litany of other illicit activity (Vogt, 2017). Over the years, the dark web has become a formalized market place for illegal goods and services, which perpetuates criminal activity. In its current state, the dark web is a protected haven for criminals to conduct illicit activities while remaining anonymous; consequently, resulting in significant spikes in crimes around the world. For example, the cost of global cybercrime totaled $400B in 2014 and forecasted to reach $6T in 2021 (Harvey, 2018). This is further corroborated by cybersecurity spending in the U.S. is forecasting a cost of $68B between 2016 and 2020 (Carter, 2017). The increasing cost of cybercrime is indicative of the ascendency of the dark web as a formalized business medium for criminals.

A salient factor of the dark web also called the black market is the use of The Onion Router (Tor), a specialized browser that provides cybercriminals anonymity by masking their identities (Chertoff, 2017). Through encrypting identity information and bundling the data packets and removing packets headers, address information, and transporting the data through several relays (layers) before reaching a destination (Vogt, 2017). The Tor was engineered and developed by the Naval Research Laboratory (NRL) at the beginning of the twenty-first century to provide the military with anonymous channels to communicate that was off the regular Internet grid (Chertoff, 2017; Vogt, 2017). In October 2003, the NRL released Tor as a free, open-source browser to increase the traffic on the dark web to increase the obscurity of military users on the dark web (Chertoff, 2017). There are 7,000 computers worldwide serving as relays, coupled with algorithms to champion the anonymity of traffic on the dark web (Chertoff, 2017). Tor is an open source tool that provides anonymity and growing audience of 2 million users per day since 2015, and often praised for enabling users to evade the U.S. surveillance efforts (Owen & Savage, 2015). Another Tor capability that aids in the increasing criminality of the dark web is hidden services, where the website host and visitors remain anonymous to each other (Owen & Savage,
Owen and Savage (2015) offered that the hidden services of the darknet allow users to operate without fear of reprisal.

There are some positive aspects of Tor such as providing users in countries with computer and website access restrictions the opportunity; internet privacy is another benefit, the proliferation of human rights from oppressive governments, and the sharing of information in privacy (Chertoff, 2017). An additional benefit of Tor is accessing the browser to gain technical and darknet experience to gain a deeper understanding of the anonymous aspect. It is critical for governments, law enforcement agencies, universities, and corporations to develop a strong comprehension of Tor’s operational capacity. Governments and military entities can use Tor as a communication node to ensure communication security regarding sensitive information.

Criminals use Tor as a manner of remaining anonymous to conduct nefarious and illicit activities. One of the first illicit activities in which Tor was used is known as the Silk Road (Yetter, 2015). The Silk Road was a full-fledged virtual e-commerce site with supporting forums, and user reviews that support anonymous exchanges between sellers and buyers (Yetter, 2015). The Silk Road was an operational e-commerce market for two and a half years before law enforcement discovered the illegal market (Yetter, 2015) which yielded profits of $1.2B in illegal sales (Ghappour, 2017). Illegal activity on the darknet ranges from the sale of counterfeit money ($600 for 2500 counterfeit dollars), compromised credit cards prices range from $5 to $80, body organs range from $1500 to $200,000, and murder for hire cost up to $180,000 (Spalevic & Ilic, 2017). According to Experian, the following items sell on the dark web (Stack, 2019):

1. Social security number - $1.00
2. Online payment services login - $20 to $200
3. Drive license - $20
4. Medical records - $1 to $1000
5. Passports - $1000 to $2000
6. Diplomas - $100 to $400

The abovementioned items illustrate the illicit activity on the dark web and the nefarious nature of the darknet, which fosters a climate of criminal behavior. Criminals have formalized the dark web into an illicit business medium due to its anonymous nature and lack of law enforcement. The ascendency of digitalization and hyperconnectivity are significant technological advances; however, both contribute to the cybercriminals increasing cyber-attacks, data breaches, and ransomware attacks. The constant attacks on corporations, business, governments, and people provide cybercriminals with an endless supply of compromised goods to sell on the dark web. The supply and demand of contraband and illegal goods on the darknet is supported by consumers seeking to purchase the illicit goods. Stack (2019) postulated that the consumer demand determines the prices of the goods and service for sell on the dark web. Interestingly, some business researchers and practitioners are exploring potential business opportunities on the dark web, which strategically signal the wrong message to criminals.

The formalization of the black market, coupled with the monetization of exfiltrated data makes cybercrime attractive and a viable market for malicious threat actors (Lewis, 2018). The lack of public information on the dark web along with the sheer size and the practice of using unindexed pages make the dark web a strategic advantage for cybercriminals. Credit card data, personally identifiable information, and other sensitive consumer data are sold on the dark web through a series of brokers and intermediate actors, primarily using digital currency to conceal identities (Lewis, 2018). Within days of Target Corporation’s data breach, millions of customer accounts and credit data were available on the dark web (Ablon, Libicki, & Golay, 2014). Given that businesses are generating, using, collecting, and storing unprecedented levels of data, criminals will increasingly target banks, hospitals, universities, and governments to gain access to large amounts of data to sell on the dark web. The uptick in cybersecurity incidents is indicative of cybercriminals attempting to exfiltrate data to engage in business exchanges on the dark web.
The dark web is becoming a new safe harbor for criminals, for example, illicit drug sale has increased on the darknet (Pergolizzi, LeQuang, Taylor, Raffa, & NEMA Research Group, 2017). According to researchers, only 4% of the internet is visible to computer users (A Dark Web Study, 2017); therefore, allowing criminals to capitalize on the vastness of the deep and dark webs. Ninety to 94% of the internet is unindexed and unconventionally accessible by regular internet users (Shining Light, 2017). Another factor is that the dark web consists of fake websites to further obfuscate criminal activity and to impeded law enforcement and to take advantage of novice dark web dwellers (A Dark Web Study, 2017). Researchers emphasized that the selling of cybersecurity weapons with malicious payloads on the darknet, primarily the availability of malware for sale is noticeable (Mirea, Wang, & Jung, 2019). It is not that the dark web is lawless, but the anonymity of the environment is complex and challenging to defeat. Nonetheless, the dark web is providing opportunities for criminals to evade capture by law enforcement agencies and formalize illegal business opportunities via the dark web.

Another concern of illicit business on the dark web is cross-border operations because countries have different laws governing unlawful activity on the Internet. Cybersecurity cross-border operations infringe on international norms but given the anonymity of the dark web, which perpetuates the use of cybercrime to formalize the darknet for a business medium (Ghappour, 2017). Cross-border operations are compounded by the lack of trained law enforcement officials and resources to reduce illicit activity on the dark web (Everett, 2015). Governments and law enforcement have to remain discreet when operating on the dark web to avert compromising their identity; consequently, pushing criminal activities deeper in the bowels of the darknet. The Tor Network is a pragmatic platform for criminal activity because traffic analysis and metadata are not supported by Tor (Ghappour, 2017). Vogt (2017) asserted that strong encryption and the robust anonymity interplay of the dark web is forcing law enforcement to leverage alternative means. However, these measures are yet to yield a consistent methodology to restrain illicit activity.

Illicit activity on the dark web requires the immediate attention of governments, corporations, and law enforcement agencies because the continuous formalizing of the dark web is ameliorating illicit business opportunities for criminals. Cases such as the Ulbright, Avalanche, and Silk Roads 2.0 and 3.0 demonstrate the illicit profitability of the darknet (Shining Light, 2017). Cybercriminals are capitalizing on the anonymous nature of the dark web resulting in increased criminal activity in forms of data breaches and cyber-attacks. At issue is the wrongful and illegitimate use of the dark web accompanied by a shortage of strategies to counter and prevent the dark web from serving business medium for criminals. One concern is forcing cybercriminals into deeper parts of the dark web, which makes it harder to detect the activity.
References


**Bio:** Dr. Nobles is a cybersecurity and information technology expert, a cybersecurity scientist, and practitioner with more than 25 years of experience. He is an adjunct faculty member at several universities teaching cybersecurity and MBA courses. He developed a Technology Management concentration for a university in California. He is active in the cybersecurity community, volunteering with multiple professional associations, conducting research and speaking at cybersecurity venues around the country. He authored a book on the integration of technologically advanced aircraft in general aviation. Dr. Nobles’ personal story is featured in the book, *Black Men Changing the Narrative Through Education*. He is a Cybersecurity Policy Fellow with the New America Think Tank in Washington, DC. He earned a Doctor of Philosophy in Management and Engineering Technology, specializing in technology innovation and integration. Dr. Nobles has earned graduate degrees in Aeronautical Science, Business Administration, and Military Strategy and Operational Art, and an undergraduate degree in Business Management. He has completed several certificates in cybersecurity from Harvard University. He is currently enrolled in the Executive Doctorate in Business Administration Program at Temple University.