Exploring the dynamics of human interactions using big data and social media: Surfacing the Cyber Underground of Darknet Markets

Daniel Z. Sui
The Ohio State University

This paper provides a synoptic overview of our on-going work is to surface and analyze the illicit cyber underground of darknet markets. By doing so, we aim to shed light on the hidden dimensions of the dynamics of human interactions using big data and social media. Darknet markets are rapidly emerging as the eBay of the underground illicit economy, providing worldwide access to hard drugs, forged documents, guns, and money laundering services, in addition to cyber-warfare tools such as phishing, spam, and botnet turnkey solutions. And yet, little is known about these emerging markets and their regulatory impact. This paper reports progress we have made on the following three tasks: (1) The data-driven analysis of 20+ existing and emerging darknet markets; (2) extraction and analysis of the supporting social network infrastructure (including thought leaders and critical hubs) through text and link analysis of darknet message forums; and (3) linking these findings to a new characterization of the regulatory challenge that emerging darknet markets present to states and the international community.

Darknet markets were popularized in the public consciousness with the spectacular rise of the Silk Road marketplace in 2011, the subsequent arrest (2013) and conviction(2015) of its owner (Ross William Ulbricht, known as the “Dread Pirate Roberts”), and the seizing of Silk Road assets by the FBI. Since then, dozens of Silk Road replacements have sprung up as *Tor hidden services*. These hidden services are deployed on the Tor network – an anonymity-providing volunteer network of thousands of Internet relays – such that users may browse these new marketplaces without worry of being tracked. Hidden services are accessed via a .onion quasi-top-level domain that is resolved through Tor. Supporting the widespread adoption of these new darknet marketplaces is the Tor Browser, a popular application for accessing Tor sites (akin to how web browsers like Chrome and Safari support access to web content), as well as the use of bitcoins for handling anonymous payments between buyers and sellers. Indeed, just as the growth of the Web “flattened” informational flows, these darknet marketplaces represent a fundamental shift in the underground illicit economy, toward enabling worldwide access and distribution of products and services that have historically required significant investments in the “last mile” of the supply chain. This disruption creates the potential for massive shifts in the international supply chain of goods and services, and particularly in illegal products.

Data-Driven Investigation. We have undertaken preliminary work towards a comprehensive data- driven analysis of existing and emerging darknet markets. Prior research into these markets has typically

focused on either a single market or on high-level trends for public consumption (e.g., press reports released by the Digital Citizens Alliance). Our goal is to conduct the first long-term study of at least 20 darknet markets. As part of this data-driven investigation, this project will create: (i) new darknet crawling techniques for surfacing the overall size of these markets in terms of products, variety of products, estimated sales numbers, and user base, in addition to cross-market comparisons on the relative success of different markets and sub-market segments, e.g., which markets are dominating the drug trade versus gun trade?; (ii) spatial-temporal analysis tools for mapping the growth of these markets, their geographic footprint (in terms of estimated buyer locations and seller locations), and product trendlines (e.g., heroin versus MDMA); and (iii) search and data mining capabilities for supporting analyst inquiries, e.g., identifying sellers with common buyer communities or finding groups of related products from different sellers that may reflect a common hidden supplier. This data-driven investigation will create the foundation for deep analysis of darknet markets and their contribution to illicit trade.

Research Thrust 2: Analyzing Supporting Social Networks. The second goal of this project is to extract and analyze the supporting social network infrastructure of these darknet marketplaces. Who are the thought leaders? Who are the critical hubs? And how do these key roles change over space and time? Many of these marketplaces include a separate discussion forum that allows pseudonymous discussions of vendor quality, site maintenance, and other issues. Through text and link analysis of these darknet message forums, this project will shed light on the size, geography, and political impacts of informal economies and illicit trade and its supply chains. By extracting pseudonyms from these forums and building on recent advances in non-negative matrix factorization and tensor decomposition, this project will uncover latent communities of interest (e.g., densely-connected participants who provide the technical know-how for maintaining these markets, groups of early adopters who shift from one market to the next, and significant “scaffolding”-like participants who provide the internal cohesion for keeping markets at a critical mass). In addition, our research findings will also offer empirical evidence on the complex links between underground markets in the cyber realm compared to their physical good counterparts in both space and time.

Research Thrust 3: Characterizing Regulatory and National Security Challenge. The third goal of this project is to understand the implications of our findings from research thrusts 1 and 2 in terms of state and international efforts to regulate and tax commercial activity (particularly but not limited to disfavored commodities such as narcotics and computer worms) and to prevent non-state actors (criminal and terrorist) and state actors from making use of darknet markets as part of activities that threaten U.S. interests. Darknet markets, by hiding the identities of those involved in transactions and often conducting business via bitcoin, inherently represent regulatory evasion. Darknet transactions involve an assortment of national crimes, from tax evasion to failure to observe duties and other limitations on imports and exports. Darknet markets also traffic heavily in contraband. One evidently common example in our information age is computer code that when utilized violates computer crime laws. In the United States, these in relevant part include the Computer Fraud and Abuse Act (CFAA), which bans trespassing on, unauthorized accessing of, and damaging computers in interstate or international commerce (see 18 1030(a)(2-5)). CFAA also bars trafficking in unauthorized computer access and computer espionage (see 18 U.S.C. 1030(a)(6)).

The international regulatory environment regarding illicit cyber activity is at an early stage of development. No treaty deals comprehensively with the cyber (in)security created in part by the availability of hacking tools via the darknet market. It is true that international law enforcement cooperation generally is longstanding and can be brought to bear on darknets and other illicit cyber activities to the extent they violate national laws and trade agreements. Law enforcement cooperation has been facilitated by the cybercrime-focused 2001 Budapest Convention (also known as the Council of Europe Convention on Cybercrime). It endeavors to harmonize criminal laws and improve investigation and cooperation among law enforcement agencies internationally on matters including computer network security, computer-related forgery and fraud, child pornography, and copyright infringements. Notably, the Convention in Article 6 states that parties shall criminalize the sale, procurement, import, and distribution of code and other hacking tools – the focus of a notable darknet market.

In the realm of international law and national security policy, there is no well-settled answer within the international community to the key questions of when a cyberattack rises to the level of an armed attack, when a cyberattack can be attributed to a state actor (particularly where the attacker masks their identity, location, and origins of the code they use in the attack, and the state from which the code was launched denies involvement), and what force used in response would be appropriate legally and operationally. The non-binding Tallinn Manual, commissioned by NATO and released in 2013, begins to address the legal element of these matters but international consensus remains elusive. In the United States, the Congress in statute and the Executive Branch in presidential guidance and other policy documents have made clear that a cyberattack – whether from a state or non-state actor using hacking tools – can rise to the level of being a use of force, and is accordingly subject to the law of armed conflict, also known as international humanitarian law or the law of war. Although diplomatic, law enforcement, and economic (regulatory) options are available in the event of a cyberattack, decisionmakers may consider as well overt or clandestine U.S. action in cyberspace by military or intelligence agencies against the darknet activities of a non-state or state actor where the information available suggests a threat to national security.