CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 6 — FEBRUARY 2015

The Impact of the Dark Web on Internet Governance and Cyber Security

Michael Chertoff and Tobby Simon

THE IMPACT OF THE DARK WEB ON INTERNET GOVERNANCE AND CYBER SECURITY

Michael Chertoff and Tobby Simon

Copyright © 2015 by the Centre for International Governance Innovation and the Royal Institute for International Affairs

Published by the Centre for International Governance Innovation and Chatham House.

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

This work is licensed under a Creative Commons Attribution — Non-commercial — No Derivatives License. To view this license, visit (www.creativecommons.org/licenses/by-nc-nd/3.0/). For re-use or distribution, please include this copyright notice.

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

4 About the Global Commission on Internet Governance

4 About the Authors

5 Executive Summary

5 Introduction

5 Context

6 The Internet, the World Wide Web and the Deep Web

7 The Dark Web

7 Cybercrime in the Dark Web

9 The Case for Online Anonymity

9 Monitoring the Dark Web

10 Conclusion

11 Works Cited

13 About CIGI

13 About Chatham House

13 CIGI Masthead

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHORS

Michael Chertoff, chairman and co-founder of the Chertoff Group and senior of counsel, Covington & Burling LLP, was secretary of the US Department of Homeland Security from 2005 to 2009. Previously, he was a US Court of Appeals judge and chief of the US Department of Justice Criminal Division. He is a magna cum laude graduate of both Harvard Law School and College. He is a commissioner with the Global Commission on Internet Governance.

The Chertoff Group is a global security advisory firm that provides consulting, business development and through Chertoff Capital, merger and acquisition advisory services for clients in the security, defense and government services industries. The Chertoff Group also advises public and private enterprises on their own physical and cyber security. With decades of trusted leadership experience across both government and financial services, the Chertoff Group advises clients on how to manage their risk, protect against a broad array of threats and crises, and grow their business within a complex security market.

Tobby Simon is president of The Synergia Foundation, an applied research think tank that works closely with academia, industry and polity to establish impactful solutions in the areas of geo-economics and geo-security. Tobby is a commissioner at the Global Commission for Internet Governance and an advisory board member of the Centre for New American Security. He is a graduate of the Harvard Business School and a research affiliate at the Massachusetts Institute of Technology. He is currently pursuing his Ph.D. at the National Institute of Advanced Studies in Bangalore, India.

The Synergia Foundation is a Bangalore-based interdisciplinary think tank that works with the industry, polity, think-tanks and academia to establish leading edge practices through applied research in the domains of geopolitics, geo-economics and geo-security. The foundation strives to help, contribute and influence public policy, private initiatives and international relations in making our region a better place for its present and future inhabitants. The foundation has over 400 years of combined experience in strategic thinking, and has multi-disciplinary teams that pursue high quality non–partisan research and draw on its global network of resources to offer the most comprehensive research analysis and impactful solutions.

IPR2025-01397
CrowdStrike EX1022 Page 6

EXECUTIVE SUMMARY

With the Internet Corporation for Assigned Names and Numbers' contract with the United States Department of Commerce due to expire in 2015, the international debate on Internet governance has been re-ignited. However, much of the debate has been over aspects of privacy and security on the visible Web and there has not been much consideration of the governance of the "deep Web" and the "dark Web."

The term deep Web is used to denote a class of content on the Internet that, for various technical reasons, is not indexed by search engines. The dark Web is a part of the deep Web that has been intentionally hidden and is inaccessible through standard Web browsers. A relatively known source for content that resides on the dark Web is found in the Tor network. Tor, and other similar networks, enables users to traverse the Web in near-complete anonymity by encrypting data packets and sending them through several network nodes, called onion routers.

Like any technology, from pencils to cellphones, anonymity can be used for both good and bad. Users who fear economic or political retribution for their actions turn to the dark Web for protection. But there are also those who take advantage of this online anonymity to use the dark Web for illegal activities such as controlled substance trading, illegal financial transactions, identity theft and so on.

Considering that the dark Web differs from the visible Web, it is important to develop tools that can effectively monitor it. Limited monitoring can be achieved today by mapping the hidden services directory, customer data monitoring, social site monitoring, hidden service monitoring and semantic analysis.

The deep Web has the potential to host an increasingly high number of malicious services and activities. The global multi-stakeholder community needs to consider its impact while discussing the future of Internet governance.

INTRODUCTION

In his advance in the Battle of the Persian Gate in 331 BC, Alexander the Great passed into the Persian Gate with little or no resistance. Convinced that he would not encounter enemy forces, Alexander neglected to send scouts ahead, and thus walked into a Persian ambush while crossing a pass on his way to Persepolis. Persian troops on either side rained boulders and arrows down on the invaders. The Macedonians suffered heavy casualties, losing entire platoons, and were forced to withdraw. Alexander then gathered intelligence from a local shepherd to encircle the Persian army in a pincer attack. His knowledge of the larger terrain helped him to outflank the Persians and emerge victorious.

Four hundred years later, seven Roman legions, some 44,000 men, marched into the searing Mesopotamian desert. They had come to the eastern province of the kingdom of Parthia seeking conquest and plunder, but, caught unaware by the uncharted terrain, the legions were almost annihilated. Most of the Romans were either slaughtered or captured and enslaved. Their commander was decapitated, and his head was used as an ornament at the banquet of the Parthian king. The Battle of Carrhae was a disaster almost unmatched in the otherwise glorious history of the Roman army. Twenty thousand were killed and 10,000 taken prisoner. It was the worst Roman defeat since the dreadful loss to Hannibal at Cannae in 216 BC. It was the result of engaging an unknown adversary, in an unknown land.

These two anecdotes remind us of the importance of reconnaissance, and the need to better understand what is beneath the surface. The deep and the dark Web can pose unseen threats. About 40 percent of the world's population uses the Web for news, entertainment, communication and myriad other purposes (International Telecommunication Union 2014). As more and more people become Internet users, they are actually finding less of the data that is stored online. Only a sliver of what we know as the World Wide Web is easily accessible.

The surface Web, which people use routinely, consists of data that search engines can find and then offer up in response to queries. This is only the tip of the iceberg — a traditional search engine sees about 0.03 percent of the information that is available (Bergman 2001). Much of the rest is submerged in what is called the deep Web. Also known as the "Undernet," "invisible Web" and the "hidden Web," it consists of data that cannot be located with a simple Google search.

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. This paper endeavours to provide a broader understanding of the dark Web and its impact on our lives.

CONTEXT

On November 3, 2014, the newly appointed director of Britain's Government Communications Headquarters, Robert Hannigan, warned that US tech giants such as Twitter, Facebook and WhatsApp have become the "command-and-control networks of choice for terrorist and criminals" (Hannigan 2014). Hannigan's statements were among the most critical of American technology firms by the head of a major intelligence agency and, more significantly, a close ally. The accusation went beyond what US officials have said so far said about Apple, Google and others that are now moving toward sophisticated

IPR2025-01397
CrowdStrike EX1022 Page 7

encryption of more and more data on phones and email systems (Wilber 2014).

This revelation was closely followed by a low-profile post by Facebook informing users that it is now hosted directly on the Tor network (Lee 2014). The Tor link — https://facebookcorewwwi.onion/ — was described more as an experiment by the company, to enable it to learn over time by providing an onion address[1] for Facebook's mobile website. Incidentally, Facebook is the first US tech giant to provide official support for Tor, a network built to allow citizens to surf the Web without being tracked and publish content that would not show up in normal search engines.

Hannigan's understanding of how the coupling of social media and the dark Web could create extremely powerful, encrypted, decentralized and anonymous propaganda networks for terrorist organizations may be what prompted him to speak out. The recent surge in the number of European nationals sympathetic to or actively supporting organizations like ISIL (the Islamic State of Iraq and the Levant) or al-Qaeda in Syria and Iraq is definitely a huge cause of worry for Western democracies. Social media platforms have proven themselves valuable recruitment tools for campaigns of all types. It is of little surprise, then, that in recent years, terrorist groups such as al-Qaeda and ISIL have successfully employed Twitter to recruit volunteers and be active in supporting their cause (Coughlin 2014). The intent is clearly to "humanize" the movement and reach broader audiences.

Beyond propaganda, cyberspace allows groups to spread particular knowledge in new and innovative ways. The kinds of tools that allow social organizations such as the Khan Academy to help kids around the world learn math and science have also given terrorist groups unprecedented ways to discuss and disseminate tactics, techniques and procedures. Recipes for explosives are readily available on the Internet and terror groups have used the Internet to share designs for improvised explosive devices instantly across conflict zones from Syria to Afghanistan (Singer 2011).

The visible side of the Internet includes sites that can be found through an ordinary search, while the invisible side — the deep Web — includes sites or networks that cannot be accessed by regular means. This includes databases, academic journals, private networks and so on. Most of the content located in the deep Web exists in websites that require a search that is not implicitly illicit. However, an intensive search will find the dark Web. The dark Web is a small portion of the deep Web that has been intentionally hidden.

While innovative methods have been developed for monitoring content on the visible Web in recent years, there are almost no similar tools for the dark Web. Providing evidence showing that the dark Web has turned into a major platform for global terrorism and criminal activities is crucial in order for the necessary tools to be developed for monitoring all parts of the Internet.

THE INTERNET, THE WORLD WIDE WEB AND THE DEEP WEB

Many people use the terms Internet and World Wide Web interchangeably, but in fact the two terms are not synonymous. The Internet and the Web are two separate but related things.

The Internet is a massive network of networks — a networking infrastructure. It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer, as long as they are both connected to the Internet.

On the other hand, the World Wide Web, or simply the Web, is a way of accessing information over the medium of the Internet. It is an information-sharing model that is built on top of the Internet. The Web uses the Hypertext Transfer Protocol, only one of the languages spoken over the Internet, to transmit data. The Internet, not the Web, is also used for email, which relies on Simple Mail Transfer Protocol, Usenet news groups, instant messaging and File Transfer Protocol. The Web, therefore, is just a portion of the Internet, albeit a large one (Beal 2010). Finally, the deep Web is, put simply, the part of the Web that is hidden from view. It is World Wide Web content that is not part of the surface Web. It cannot be accessed by normal search engines. This massive subsection of the Internet is more than 500 times bigger than the visible Web (Barker and Barker 2013).

1 An onion address designates an anonymous hidden service reachable via the Tor network.

IPR2025-01397
CrowdStrike EX1022 Page 8

Deep Web Resources:

- Dynamic content
- Unlinked content
- Private Web
- Contextual Web
- Limited access content

Accessing the Deep Web:

- Custom Web crawlers use key terms provided by users or collected from the query interfaces to query a Web form and crawl the deep Web resources.
- Commercial search engines have begun exploring alternative methods to crawl the deep Web. The Sitemap Protocol (first developed and introduced by Google in 2005) is a mechanism that allows search engines and other interested parties to discover deep Web resources on particular Web servers (Google 2014).

THE DARK WEB

The dark Web is the portion of the deep Web that has been intentionally hidden and is inaccessible through standard Web browsers. Dark Web sites serve as a platform for Internet users for whom anonymity is essential, since they not only provide protection from unauthorized users, but also usually include encryption to prevent monitoring.

A relatively known source for content that resides on the dark Web is found in the Tor network. The Tor network is an anonymous network that can only be accessed with a special Web browser, called the Tor browser (Tor 2014a). First debuted as The Onion Routing (Tor) project in 2002 by the US Naval Research Laboratory, it was a method for communicating online anonymously. Another network, I2P, provides many of the same features that Tor does. However, I2P was designed to be a network within the Internet, with traffic staying contained in its borders. Tor provides better anonymous access to the open Internet and

I2P provides a more robust and reliable "network within the network" (Tchabe and Xu 2014).

USAGE

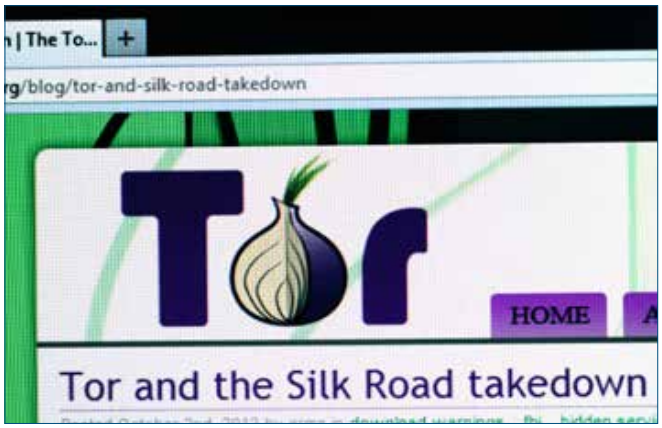
The ability to traverse the Internet with complete anonymity nurtures a platform ripe for what are considered illegal activities in some countries, including:

- controlled substance marketplaces;
- credit card fraud and identity theft; and
- leaks of sensitive information.

Silk Road was an online marketplace that dealt with contraband drugs, narcotics and weapons. In 2013, the US Federal Bureau of Investigation (FBI) shut down the website. But like the mythical Hydra, the website resurrected as Silk Road 2.0 within a month. It took the FBI another year to track down its administrator and servers (Mac 2014).

It should also be noted that Tor empowers anyone who wants control over his or her online footprint. The positive value of such a tool is huge for some groups, such as whistle-blowers who report news that companies would prefer to suppress, human rights workers struggling against repressive governments and parents trying to create a safe way for their children to explore the Web.

IPR2025-01397
CrowdStrike EX1022 Page 9



A Tor Project website blog page discussing the takedown of Silk Road (an online marketplace that dealt with contraband drugs, narcotics and weapons) by the FBI. iStock.

DEFINING ATTRIBUTES

Anonymity, from the Greek word *anonymia*, refers to the state where one's personal identity is not publicly known. Each day, our Web actions leave footprints by depositing personal data on the Internet. This information composes our digital identity — our representation in cyberspace.

Internet anonymity is guaranteed when Internet Protocol (IP) addresses cannot be tracked. Tor client software routes Internet traffic through a worldwide volunteer network of servers, hiding user's information and eluding any activities of monitoring. This makes the dark Web very appropriate for cybercriminals, who are constantly trying to hide their tracks (Paganini 2012).

The dark Web is also the preferred channel for governments to exchange documents secretly, for journalists to bypass censorship of several states and for dissidents to avoid the control of authoritarian regimes (Gehl 2014). Anonymous communications have an important place in our political and social discourse. Many individuals wish to hide their identities due to concerns about political or economic retribution.

Onion routing is a technique for anonymous communication over a computer network. Messages are repeatedly encrypted and then sent through several network nodes, called onion routers. Like someone peeling an onion, each onion router removes a layer of encryption to uncover routing instructions, and sends the message to the next router, where the process is repeated. This technique prevents intermediary nodes from knowing the origin, destination and contents of the message (Tor 2014a).

CYBERCRIME IN THE DARK WEB

Peter Grabosky (2001) notes that virtual crime is not any different than crime in the real world — it is just executed in a new medium: "'Virtual criminality' is basically the same as the terrestrial crime with which we are familiar. To be sure, some of the manifestations are new. But a great deal of crime committed with or against computers differs only in terms of the medium. While the technology of implementation, and particularly its efficiency, may be without precedent, the crime is fundamentally familiar. It is less a question of something completely different than a recognizable crime committed in a completely different way."

DRUGS, WEAPONS AND EXOTIC ANIMALS

Websites such as Silk Road act as anonymous marketplaces selling everything from tame items such as books and clothes, to more illicit goods such as drugs and weapons. Aesthetically, these sites appear like any number of shopping websites, with a short description of the goods, and an accompanying photograph (Bartlett 2014).

STOLEN GOODS AND INFORMATION

It is correct to assume that dedicated sites facilitate users to trade in both physical and proprietary information, including passwords and access to passwords for surface Web paid-pornography sites and PayPal passwords (Westin 2014). PayPal Store, Creditcards for All and (Yet) Another Porn Exchange are active websites that offer such services.

MURDER

The Assassination Market website is a prediction market where a party can place a bet on the date of death of a given individual, and collect a payoff if the date is "guessed" accurately. This incentivizes the assassination of individuals because the assassin, knowing when the action will take place, could profit by making an accurate bet on the time of the subject's death. Because the payoff is for knowing the date rather than performing the action of the assassination, it is substantially more difficult to assign criminal liability for the assassination (Greenberg 2013). There are also websites to hire an assassin — popular ones are White Wolves and C'thuthlu (Pocock 2014).

TERRORISM

The dark Web and terrorists seem to complement each other — the latter need an anonymous network that is readily available yet generally inaccessible. It would be hard for terrorists to keep up a presence on the surface Web because of the ease with which their sites could be shut down and, more importantly, tracked back to the original poster.

IPR2025-01397
CrowdStrike EX1022 Page 10

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.

HACKTIVISM

More radical critics and hacktivists occupy part of the political dissidence space. The group Anonymous, commonly associated with Occupy Wall Street and other cyber activism, is one prominent hacktivist group (Jones 2011).

EXPLOIT MARKETS

Exploits are malware based on software's vulnerabilities — before they are patched. Zero-day exploits target zero-day vulnerabilities — those for which no official patch has been released by the vendor. "Zero-day" refers to the fact that the programmer has had zero days to fix the flaw. Exploit markets serve as platforms for buying and selling zero-day exploits, and an exploit's price factors in how widely the target software is used as well as the difficulty of cracking it (Miller 2007).

> "One of the things driving the rapid rise in cybercrime is that the cybercriminal does not have to be a master hacker since the exploits can be bought."
>
> *Sir David Bruce Omand, GCB*

ILLEGAL FINANCIAL TRANSACTIONS

Websites such as Banker & Co. and InstaCard facilitate untraceable financial transactions through various methods. They either launder bitcoins by disguising the true origin of the transactions or give users an anonymous debit card issued by a bank. Users are also given virtual credit cards issued by trusted operators in the dark Web (Dean 2014).

Buying stolen credit card information has never been easier. A website called Atlantic Carding offers this service, and the more you pay, the more you get. Up for grabs are business credit card accounts and even infinite credit card accounts associated with ultra-high-net-worth individuals. The user's details — name, address and so on — are available at an additional cost (Dahl 2014).

THE HIDDEN WIKI

The main directory on the dark Web is the Hidden Wiki. It also promotes money laundering services, contract killing, cyber attacks and restricted chemicals, along with instructions to make explosives. As with other dark Web sites, the links to these sites frequently change to evade detection (Williams 2011).

HUMAN EXPERIMENTATION

The Human Experiment was a website that detailed medical experiments claimed to have been performed on homeless people who were usually unregistered citizens. According to the website, they were picked up off the street, experimented on and then usually died. The website has been inactive since 2011 (Falconer 2012).

HEIST

There are many rob-to-order pages available in the dark Web, hosted by people who are good at stealing and will steal anything that you cannot afford or just do not want to pay for (Siddiqui 2014).

ARMS TRAFFICKING

Euroarms is a website that sells all kinds of weapons that can be delivered to your doorstep anywhere in Europe. The ammunition for these weapons is sold separately — that website has to be tracked down separately on the dark Web (Love 2013).

GAMBLING

Many popular bitcoin gambling sites block US IPs because they are afraid of prosecution from the United States, which has a tight hand on gambling in the United States. With the help of the dark Web, users of these sites can continue gambling by disguising their US IP (O'Neill 2013).

PEDOPHILIA

Pedophilia, or CP (for child pornography) as it is commonly referred to on the dark Web, is extremely accessible. Pornography is accepted on the surface Web with some regulation. The dark Web offers various types of sites and forums for those wishing to engage in pedophilia (Greenberg 2014).

THE CASE FOR ONLINE ANONYMITY

Like any technology, anonymity can be used for both good and bad purposes. Many people do not want the things they say online to be connected with their offline identities. They may be concerned about political or economic retribution, harassment or even threats to their lives. Instead of using their true names to communicate, these people choose to speak using pseudonyms or

IPR2025-01397
CrowdStrike EX1022 Page 11

anonymously. Listed below are a few scenarios where users turn to the online anonymity provided by Tor (Tor 2014b).

Civilians

- protection of privacy from unscrupulous marketers and identity thieves
- protection of communications from irresponsible corporations
- protection of children online
- to research sensitive topics
- to circumvent censorship

Militaries

- field agents
- hidden services of command and control
- intelligence gathering

Journalists and Their Audience

- to help Internet users in countries without safe access to free media
- to write about local events to encourage social change and political reform
- to avoid risking the personal consequences of intellectual curiosity

Law Enforcement

- online surveillance
- sting operations
- maintaining anonymous tip lines

Activists and Whistle-blowers

- to report abuses from danger zones
- anonymous blogging
- to speak out about government corruption

For these individuals and the organizations that support them, secure anonymity is critical. It may literally save lives. While the undesired effects of Tor must be recognized, the complexities and varied situations should make us suspicious of sweeping imperatives. Policies should be crafted to specific contexts (Marx 1999).

MONITORING THE DARK WEB

The dark Web, in general, and the Tor network, in particular, offer a secure platform for cybercriminals to support a vast amount of illegal activities — from anonymous marketplaces to secure means of communication, to an untraceable and difficult to shut down infrastructure for deploying malware and botnets.

As such, it has become increasingly important for security agencies to track and monitor the activities in the dark Web, focusing today on Tor networks, but possibly extending to other technologies in the near future.

Due to its intricate webbing and design, monitoring the dark Web will continue to pose significant challenges. Efforts to address it should be focused on the areas discussed below (Ciancaglini et al. 2013).

MAPPING THE HIDDEN SERVICES DIRECTORY

Both Tor and I2P use a domain database built on a distributed system known as a "distributed hash table," or DHT. A DHT works by having nodes in the system collaboratively take responsibility for storing and maintaining a subset of the database, which is in the form of a key-value store. Due to the distributed nature of the hidden services domain resolution, it is possible to deploy nodes in the DHT to monitor requests coming from a given domain.

CUSTOMER DATA MONITORING

Security agencies could benefit from analyzing customer Web data to look for connections to non-standard domains. Depending on the level of Web usage at the customer side, this may not help in tracking down links to the dark Web, but it may still provide insights on activities hosted with rogue top-level domains. This can be done without intruding on the user's privacy as only the destinations of the Web requests need to be monitored and not who is connecting to them.

SOCIAL SITE MONITORING

Sites such as Pastebin are often used to exchange contact information and addresses for new hidden services. These sites would need to be kept under constant observation to spot message exchanges containing new dark Web domains.

HIDDEN SERVICE MONITORING

Most hidden services to date tend to be highly volatile and go offline very often, coming back online later under a new domain name. It is essential to get a snapshot of every new site as soon as it is spotted, for later analysis or to monitor

IPR2025-01397
CrowdStrike EX1022 Page 12

its online activity. While crawling the clear Internet is usually an operation involving the retrieval of resources related to a site, this is not recommended in the dark Web. There is the possibility of automatically downloading content such as child pornography, the simple possession of which is considered illegal in most countries.

SEMANTIC ANALYSIS

Once the data for a hidden service (any of the websites on the dark Web) is retrieved, building a semantic database that contains important information about a hidden site can help track future illegal activities on the site and associate them with malicious actors.

MARKETPLACE PROFILING

Finally, it would be helpful to focus on profiling transactions made on dark Web marketplaces to gather information about sellers, users and the kinds of goods exchanged. Individual profiles could be built up over time.

CONCLUSION

The deep Web — in particular, networks on the dark Web such as Tor — represents a viable way for malicious actors to exchange goods, legally or illegally, in an anonymous fashion.

The lack of observable activities in unconventional dark Web networks does not necessarily mean they do not exist. In fact, in agreement with the principle that inspires the dark Web, the activities are simply more difficult to spot and observe. A driving factor for the marketplace is critical mass. Operators in the dark Web are unlikely to need a high level of stealth unless the consequences, if they are discovered, are sufficiently severe. It is conceivable that sites may come online at specific times, have a brief window of trading, then disappear, making them more difficult to investigate.

Recent revelations about wide-scale nation-state monitoring of the Internet and recent arrests of cybercriminals behind sites hosted in the dark Web are starting to lead to other changes. It would not be surprising to see the criminal underbelly becoming more fragmented into alternative dark nets or private networks, further complicating the job of investigators.

The dark Web has the potential to host an increasingly large number of malicious services and activities and, unfortunately, it will not be long before new large marketplaces emerge. Security researchers have to remain vigilant and find new ways to spot upcoming malicious services to deal with new phenomena as quickly as possible.

WORKS CITED

Barker, Donald I. and Melissa Barker. 2013. *Internet Research Illustrated*. Independence, KY: Cengage Learning, C-4.

Bartlett, Jamie. 2014. "Dark Net Markets: The eBay of Drug Dealing," *The Observer*, October 5.

Beal, Vangie. 2010. "The Difference between the Internet and World Wide Web." Webopedia, June 24.

Bergman, Michael K. 2001. "White Paper: The Deep Web: Surfacing Hidden Value." http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main.

Ciancaglini, Vincenzo, Marco Balduzzi, Max Goncharov and Robert McArdle. 2013. "Deepweb and Cybercrime: It's Not All About TOR." Trend Micro Research Paper. October.

Coughlin, Con. 2014. "How Social Media Is Helping Islamic State to Spread Its Poison." *The Telegraph*, November 5.

Dahl, Julia. 2014. "Identity Theft Ensnares Millions while the Law Plays Catch Up." CBS News, July 14.

Dean, Matt. 2014. "Digital Currencies Fueling Crime on the Dark Side of the Internet." Fox Business, December 18.

Falconer, Joel. 2012. "A Journey into the Dark Corners of the Deep Web." The Next Web, October 8.

Gehl, Robert W. 2014. "Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network." New Media & Society, October 15. http://nms.sagepub.com/content/early/2014/10/16/1461444814554900.full#ref-38.

Google. 2014. "Learn about Sitemaps." ps://support.google.com/webmasters/answer/156184?hl=en.

Grabosky, Peter. 2001. "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies* 10: 243–49. http://sls.sagepub.com/content/10/2/243.full.pdf.

Greenberg, Andy. 2013. "Meet the 'Assassination Market' Creator Who's Crowdfunding Murder with Bitcoins." Forbes, November 18.

———. 2014. "Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds." *Wired*, December 30.

Hannigan, Robert. 2014. "The Web Is a Terrorist's Command-and-Control Network of Choice." *The Financial Times*, November 3.

IPR2025-01397
CrowdStrike EX1022 Page 13

International Telecommunication Union. 2014. "The World in 2014: ICT Facts and Figures." www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf.

Jones, Melanie. 2011. "Anonymous NYSE: Wall Street 'Hacktivism' Exposes Downside of Anonymity." *International Business Times*, October 11.

Lee, David. 2014. "Facebook Sets Up 'Dark Web' Link to Access Network via Tor." BBC, November 3.

Love, Dylan. 2013. "There's a Secret Internet for Drug Dealers, Assassins, and Pedophiles." *Business Insider*, March 6.

Mac, Ryan. 2014. "Feds Shutter Illegal Drug Marketplace Silk Road 2.0, Arrest 26-Year-Old San Francisco Programmer." *Forbes*, November 6.

Marx, Gary T. 1999. "What's in a Name? Some Reflections on the Sociology of Anonymity." http://web.mit.edu/gtmarx/www/anon.html.

Miller, Charlie. 2007. "The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales." http://weis2007.econinfosec.org/papers/29.pdf.

O'Neill, Patrick Howell. 2013. "Inside the Bustling, Dicey World of Bitcoin Gambling." The Daily Dot, December 17.

Paganini, Pierluigi. 2012. "The Good and the Bad of the Deep Web." Security Affairs, September 17.

Pocock, Zane. 2014. "How to Navigate the Deep Web." *Critic*, Issue 03, March 19.

Siddiqui, Sameer Iqubal. 2014. "Real Power of Deep Web and How to Harness It." *Real Hackers Point* (blog), June 19.

Singer, Peter W. 2012. "The Cyber Terror Bogeyman." November 2012. The Brookings Institution. www.brookings.edu/research/articles/2012/11/cyber-terror-singer.

Tchabe, Gildas Nya and Yinhua Xu. 2014. "Anonymous Communications: A Survey on I2P." www.cdc.informatik.tudarmstadt.de/fileadmin/user_upload/Group_CDC/Documents/Lehre/SS13/Seminar/CPS/cps2014_submission_4.pdf.

Tor Project. 2014a. "Tor: Overview." www.torproject.org/about/overview.html.en.

———. 2014b. "Inception." www.torproject.org/about/torusers.html.en.

Westin, Ken. 2014. "Stolen Credit Cards and the Black Market: How the Deep Web Underground Economy Works." LinkedIn, August 22.

Wilber, Del Quentin. 2014 "U.S. Law Enforcement Seeks to Halt Apple-Google Encryption of Mobile Data." Bloomberg News, September 30.

Williams, Christopher. 2011. "The Hidden Wiki: An Internet Underworld of Child Abuse." *The Daily Telegraph*, October 27.

IPR2025-01397
CrowdStrike EX1022 Page 14

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

ABOUT CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI MASTHEAD

Managing Editor, Publications	Carol Bonnett
Publications Editor	Jennifer Goyder
Publications Editor	Vivian Moser
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Graphic Designer	Melodie Wakefield
Graphic Designer	Sara Moore

EXECUTIVE

President	Rohinton Medhora
Vice President of Programs	David Dewitt
Vice President of Public Affairs	Fred Kuntz
Vice President of Finance	Mark Menard

COMMUNICATIONS

Communications Manager	Tammy Bender	tbender@cigionline.org (1 519 885 2444 x 7356)

CIGI PUBLICATIONS
ADVANCING POLICY IDEAS AND DEBATE

The Regime Complex for Managing Global Cyber Activities

GCIG Paper Series No. 1
Joseph S. Nye, Jr.

When trying to understand cyber governance, it is important to remember how new cyberspace is. Advances in technology have, so far, outstripped the ability of institutions of governance to respond. This paper concludes that predicting the future of the normative structures that will govern cyberspace is difficult.

Legal Interoperability as a Tool for Combatting Fragmentation

GCIG Paper No. 4
Rolf H. Weber

The recently developed term "legal interoperability" addresses the process of making legal rules cooperate across jurisdictions. It can facilitate global communication, reduce costs in cross-border business and drive innovation, thereby creating a level playing field for the next generation of technologies and cultural exchange.

Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate

GCIG Paper Series No. 2
Tim Maurer and Robert Morgus

This paper offers an analysis of the global swing states in the Internet governance debate and provides a road map for future in-depth studies.

Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem

GCIG Paper No. 5
Stefaan G. Verhulst, Beth S. Noveck, Jillian Raines and Antony Declercq

The growth and globalization of the Internet over the past 40 years has been nothing short of remarkable. Figuring out how to evolve the Internet's governance in ways that are effective and legitimate is essential to ensure its continued potential.

Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-stakeholder Community

GCIG Paper No. 3
Aaron Shull, Paul Twomey and Christopher S. Yoo

Under the existing contractual arrangement, the Internet Corporation for Assigned Names and Numbers (ICANN) has been accountable to the US government for the performance of these functions. However, if the US government is no longer party to this agreement, then to whom should ICANN be accountable?

Finding Common Ground: Challenges and Opportunities in Internet Governance and Internet-related Policy

Briefing Book
CIGI Experts

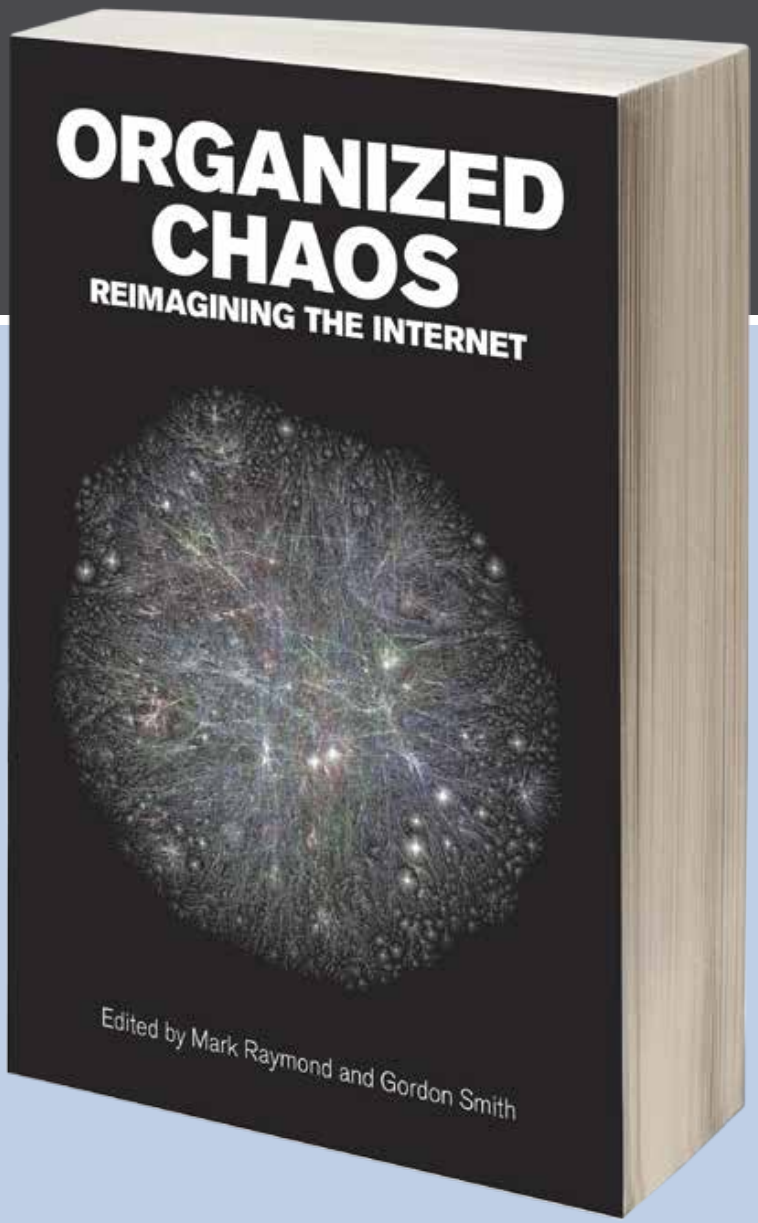
This briefing book contextualizes the current debate on the many challenges involved in Internet governance. These include managing systemic risk — norms of state conduct, cybercrime and surveillance, as well as infrastructure protection and risk management; interconnection and economic development; and ensuring rights online — such as technological neutrality for human rights, privacy, the right to be forgotten and the right to Internet access.

Available as free downloads at www.cigionline.org

ORGANIZED CHAOS
REIMAGINING THE INTERNET

EDITED BY

MARK RAYMOND AND GORDON SMITH



Leading experts address a range of pressing challenges, including cyber security issues and civil society hacktivism by groups such as Anonymous, and consider the international political implications of some of the most likely Internet governance scenarios in the 2015-2020 time frame. Together, the chapters in this volume provide a clear sense of the critical problems facing efforts to update and redefine Internet governance, the appropriate modalities for doing so, and the costs and benefits associated with the most plausible outcomes. This foundation provides the basis for the development of the research-based, high-level strategic vision required to successfully navigate a complex, shifting and uncertain governance environment.

Price: CDN$25.00
200 Pages, Trade Paperback
ISBN 978-1-928096-04-7

CIGI

Centre for International Governance Innovation

Single copy orders: cigionline.org/bookstore
Available in paperback and e-book form.

67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org