REFINING THE NET IMPACT OF ONION ROUTING TECHNOLOGY

An STS Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

By
VINEET KALPATHI

Spring 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature VINEET KALPATHI Date _____
Vineet Kalpathi

Approved _____ Date _____
Richard Jacques, Department of Engineering and Society

INTRODUCTION

The world's unfaltering use and extensive dependence on the internet has resulted in a wide variety of mechanisms used to target and surveil users, websites, or entire organizations online. This heightened tracking of internet activity stems from a plethora of motives, including marketing schemes, government surveillance, or malicious cyberattacks on a specific entity. The increased vulnerability of user privacy on the internet is largely attributable to the well-known protocols that our internet has been running on since its inception. For example, a compromised encryption key could allow a malicious user to intercept messages en route from sender to receiver and easily decode an encrypted message, subsequently identifying both parties involved and the data sent between them. Given the importance of many present-day processes that rely on the internet, attacks on privacy could potentially have grave consequences depending on the nature of the communication. This identifies a need for a routing protocol that could prevent such large-scale monitoring of internet activity.

The Onion Router (TOR), also known as anonymity network or the dark web, is a system of both software and hardware dedicated to providing users with a completely anonymous way to browse the internet. Backed by a network of volunteered servers (also known as relays or nodes), TOR provides anonymity to users by implementing an internet routing protocol called 'onion routing.' Unlike ordinary protocols, onion routing intentionally obfuscates transmitted messages through layered, asymmetric encryption, thus preventing any outsider from discerning a message's source, destination, or content.

When a client wants to communicate with a server on TOR, the protocol first establishes a connection between the two parties by defining an *onion*, or a random path of relays and each relay's relevant cryptographic information. Using the public keys of every node along the circuit,

the sender encrypts the message multiple times in layers, such that each node along the message's path can only decrypt a single layer of the message—much like the peeling of an onion. Each decryption during the message's journey only reveals the identity of the next node along the path, ensuring that only the destination relay can decode the true message, and that each intermediate relay only knows its immediate neighbors along the route; therefore, the identities of the true source and destination of every message on the TOR network are hidden (Goldschlag, Reed, & Syverson, 1999, p. 2).

By establishing these secure connections that prevent both packet sniffing and traffic analysis, onion routing grants anonymity to both clients and servers on the TOR network, allowing for the existence of hidden services accessible only through TOR. These anonymity-providing systems allow hidden sites to enable the proliferation of cybercrime such as illegal markets and pedophilia rings; however, in an age of increased internet censorship, data mining, and surveillance, such systems also grant users with increased security, privacy, and freedom while surfing the web. This makes the anonymity network a double-edged sword, having both favorable and unfavorable characteristics that are often contested. In this paper, I argue that the most feasible solution to attenuate the effects of cybercrime on TOR while allowing the promotion of privacy and democracy is to actively police the anonymity network. Although establishing an online policing institution demands thorough rumination to preserve the existing rights of individuals online and the functionality of modern internet infrastructure, the benefits of the onion-routing network for a growing population of internet users concerned about their privacy are difficult to ignore.

THE INTERPRETIVE FLEXIBILITY OF THE DARK WEB

The empowering character of anonymity-granting systems makes technologies like TOR inherently political. Media coverage often focuses on the gruesome cybercrime that occurs on the dark web, such as law enforcement's crackdown on child pornography site Freedom Hosting and the largest online anonymous illegal market, the Silk Road—two of the dark web's most prominent hidden services (Weimann, 2016). The Silk Road, owned by Ross Ulbricht—previously known by the pseudonym 'Dread Pirate Roberts'—began its operations in February 2011, connecting merchants selling a wide range of illegal goods and services with interested buyers. Items on the site ranged anywhere from drugs, to stolen identities, to assassinations-for-hire. Upon receiving intelligence about this marketplace from an informant, the Department of Homeland Security (DHS) initiated an undercover investigation that eventually resulted in Ulbricht's arrest and the shutdown of the hidden service in October 2013. Nevertheless, two more generations of the site have replaced the initial service to fulfill the demand of criminals worldwide (Christin, 2012). The tendency for the dark web to enable cybercriminals naturally creates antipathy towards TOR, regardless of the online privacy and freedom that it grants internet users around the world.

After the uncovering of the National Security Administration's (NSA) mass surveillance programs and the overwhelming skepticism around big tech, the public has become increasingly concerned about their privacy while surfing the internet. The onion-routing network offers peace-of-mind to those perturbed about being constantly tracked online, given its ability to sever the link between an internet user and their online activity. However, the greatest avails of TOR are seen among politically active citizens of repressive regimes, where unrestrained internet access is often curtailed.

The dark web is not typically associated with its ability to foster democracy, albeit the network's originally intended purpose. Under the protective shadow of anonymity, oppressed individuals are able to bypass censorship, voice opinions against the majority, and communicate directly with journalists and political activists globally. Media generally fails to shine light on TOR's ability to aid the oppressed—for example, in helping Syrian families communicate and survive in war-torn areas like Homs (Borland, 2013). Needless to say, TOR's diverse usage is largely dependent on the regimes that users reside within.

Jardine (2018) exhibits a consistent, U-shaped association between political structure and TOR usage, suggesting that "repression [drives] usage of Tor the most in … highly liberal and highly repressive contexts and the least in partly free countries." The opportunity—or lack thereof—that individuals are granted by political regimes directly affects how TOR is used, observing the highest rates of cybercrime in democratic countries and the highest rates of political activism in more restrictive countries (Jardine, 2015, p. 4). Using the Technology and Social Relationships model (Carlson, 2007, p. 3), Figure 2 maps the prominent relationships between TOR-using citizens and regimes of both authoritarian and democratic nature.

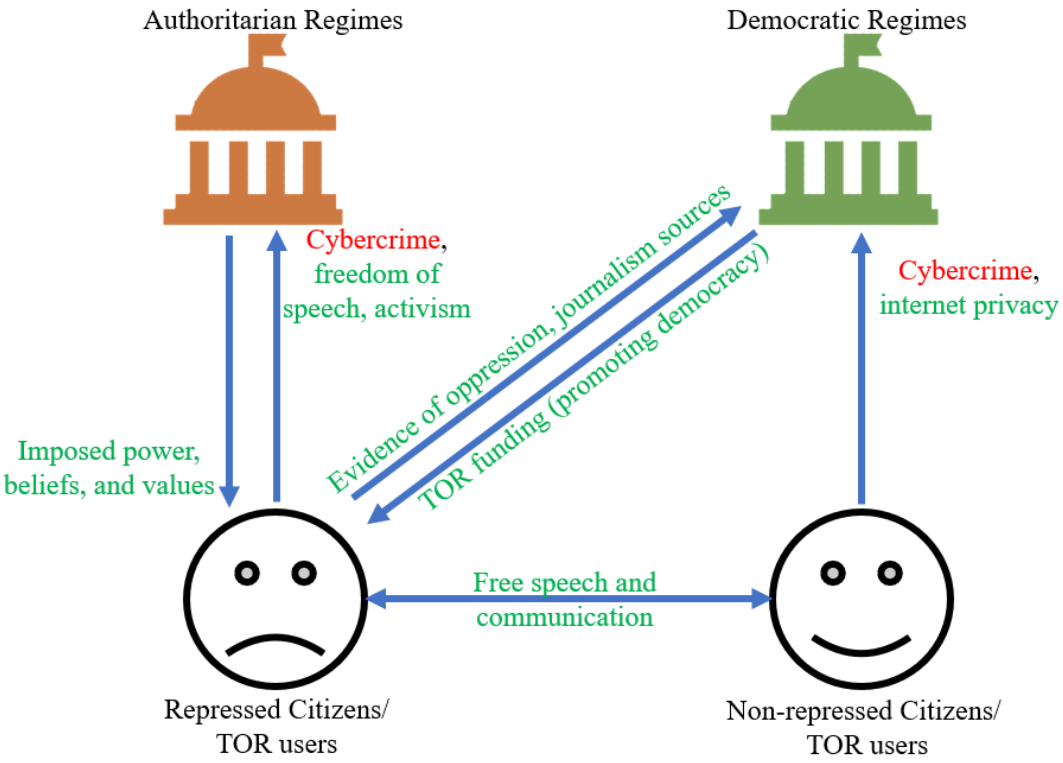

Figure 2: A Sociotechnical View of Relationships between TOR Users and National Regimes. A depiction of the relevant interactions between regimes and TOR-using citizens. Negative impacts are shown in red, while positive impacts are shown in green. (Kalpathi, 2020).

It can be observed that much of TOR's utilization is beneficial, given its widespread promotion of democracy. Nevertheless, the overwhelming presence of cybercrime on the network continues to outshine the advantages, giving rise to conversations about putting an end to anonymity-granting networks. How can TOR shake its evil reputation and begin to be known for its tremendous avails?

MITIGATING CYBERCRIME ON THE ANONYMOUS NETWORK

Given the prevalence of cybercrime on the anonymous network, it is reasonable to expect that TOR's net effect could be improved by attacking the ability of users to conduct illegal activity through the dark web. However, any attempt to destroy or shut down the encrypted network would be ineffective, as the prevalence of TOR's user base suggests that there is an

inevitable demand for anonymity-granting systems, and a new anonymous network would likely replace the onion router.

Additionally, onion routing technology is only in charge of regulating how data is transmitted on the internet to provide anonymity for the user, and largely unconcerned with how users leverage this technology. If developers were to modify TOR with the intention of identifying cybercriminals, they would simultaneously be working to aid oppressive regimes in identifying which citizens are acting out of line. For instance, the implementation of a back door for law enforcement to easily identify and pursue cybercriminals on the anonymous network would simply create a vulnerability to be exploited by anybody—including authoritarian governments in their pursuit against subjugated individuals voicing their opinions, or communicating with journalists in more liberal nations. Any such feature would render the technology insecure, and ultimately useless. Given that repressed citizens and cybercriminals both benefit from the anonymity of TOR, any development to onion routing technology will have a negligible effect on its ultimate impact.

As shown in Figure 3, Pacey's Triangle of Technology Practice (Pacey, 1983, p. 6) identifies two more potential realms of modification towards mitigating cybercrime on TOR: the cultural and organizational domains of influence. The figure demonstrates the larger network that onion routing technology is embedded within. Pursuing a change in culture to mitigate the malice of TOR would suggest changing the very nature of authoritarianism and democracy, or alternatively, the mindset and motives of cybercriminals; the world would be a much more benevolent place if humans had this power. Any modification to aid in improving the dark web's net impact should therefore be an organizational concern—primarily a change in institutions and policy.

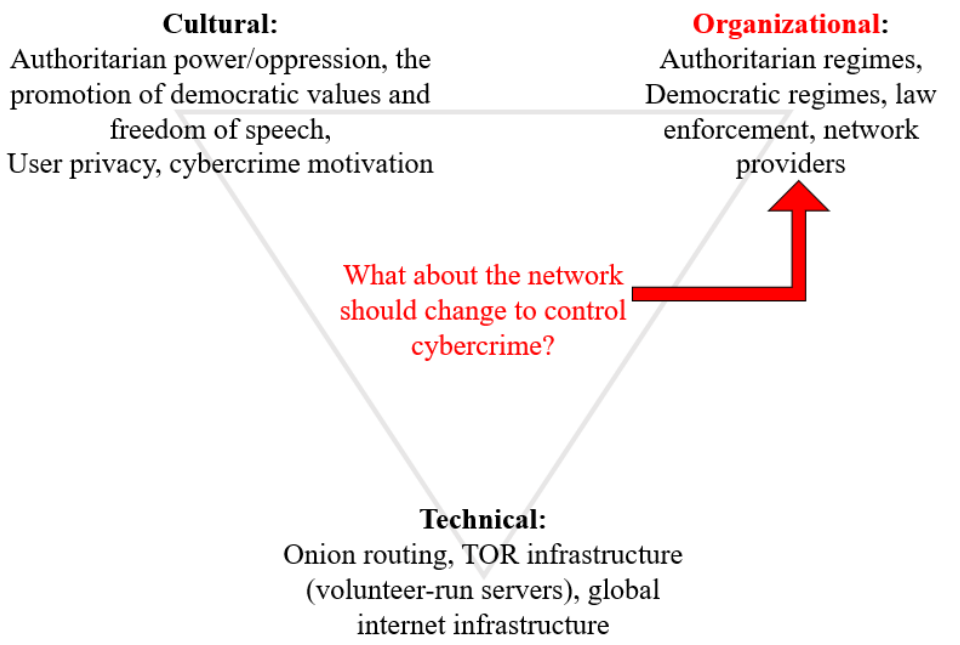

Figure 3: The Onion Router in the Context of Pacey's Triangle. This illustration highlights the cultural, organizational, and technical aspects of the network surrounding TOR and its users (Kalpathi, 2020).

As suggested by the figure above, the most feasible approach to prevent the proliferation of illegal activity on TOR would be to propose a change to institutional aspects of the larger social network in which the anonymity network resides.

A reasonable solution to control cybercrime while allowing repressed citizens to practice internet freedom would be to actively police the TOR network, but the application of new institutions and policy requires several considerations to ensure that existing organizational, cultural, and technological systems are not broken. These concerns elucidate the complexity of implementing such a modern institution, and the lack of practical examples available in the sphere of internet governance.

CONSIDERATIONS FOR THE ADMINISTRATION OF AN ONLINE POLICING INSTITUTION

As cyberspace continues to grow at an exponential rate, it is vital for societies to invest in institutions to uphold the law online. Unfortunately, many well-accepted policies regarding

traditional law enforcement fall flat when applied to the domain of cyberspace. Perhaps the most obvious issue is the sheer growth required for law enforcement agencies to train officials on cybercrime and the appropriate methods of online investigations. Police academy curriculums would have to be radically transformed to include training for investigating cases of cybercrime. Pursuing criminals on the anonymity network would require even more rigorous technical training in order to successfully and legally track down hidden criminals. Adapting police education to include cybercrime training would consequently be a costly affair, likely infeasible for the limited budgets of local enforcement agencies. Investigating cybercrime would need to be passed to wealthier divisions of government, such as national or multinational agencies.

Another concern for online policing is determining whose jurisdiction a cybercrime falls under. Policing crimes across borders is a complicated matter—one that is much further complicated when crimes are committed on the global infrastructure of the internet. Although a criminal could be operating from his own home in one location, the computer on which the crime is being processed could be in a completely separate location, potentially across the world. Mutual legal assistance treaties (MLATs) are mechanisms that allow for law enforcement agencies to tackle criminals across borders by sharing evidence. The policy is in serious need of reform, given the tedious, drawn out process of obtaining access to cross-border law enforcement data; however, any hastened refinements to MLAT legislation can certainly result in overly accessible data, cultivating the possibility of global state surveillance by federal entities (Galvagna 2019). In addition, not all countries support MLATs, further complicating the issue of cybercrime jurisdiction (Woods, 2015). Countries involved in cybercrime investigations would need to fully agree on what is illegal and what is not, a task that is much easier done between liberal democratic countries than between politically divergent regimes that fundamentally

disagree on many legislative values (Jardine, 2015). The challenging aspects of international collaboration could certainly be exploited by cybercriminals to provide protection while plotting their schemes.

Another important contingency is the ambiguity around enforcement regulations, encouraging the warrant-based monitoring of hidden illegal websites on top of existing internet infrastructure to avoid illegal breaches of privacy and the destruction of internet technology. Although getting trained professionals to hack into a website would be a quick and easy method to obtain evidence against an alleged cybercriminal on TOR, this is still a breach of privacy and a violation of the fourth amendment. Hacking into the systems of suspected criminals without a warrant is an illegal means to obtain evidence, just as is breaking into a suspect's home. Online policing should therefore involve undercover operations in order to lawfully obtain evidence against criminals. The aforementioned arrest of Ulbricht and the takedown of the Silk Road exemplify a successful, legal investigation in the pursuit of cybercriminals on the onion-routing network.

CONCLUSION

Although the dark web is infamous for enabling gruesome cybercrime on the network, the potential for anonymity-granting systems like TOR to improve the privacy of internet users in both democratic and authoritarian regimes calls for a solution to mitigate its ravages. This paper has argued that establishing an institution to actively police these networks would be the most feasible option to rid such systems of the malice of cybercrime while preserving their ability to promote internet privacy and democratic values such as free speech and anti-censorship. Given the many concerns in establishing an organization to police the dark web, multiple democratic nations must

band together to establish an institution to target cybercriminals. Implementing a centralized, multinational law enforcement agency dedicated to cybercrime would allow multiple governments to pool their monetary wealth, knowledge, and technical skills in creating effective policy to legally attack unlawful activity on TOR, thus promoting the privacy-improving, democracy-fostering uses of onion routing technology.

REFERENCES

Borland, J. (2013, December 28) For tor, publicity a mixed blessing. *Wired*. Retrieved from http://www.wired.com/2013/12/tor-publicity-mixed-blessing/

Bradshaw, S., DeNardis, L. (2015). The emergence of contention in global internet governance. *Global Commission on Internet Governance Paper Series*, 17.

Carlson, W. (2007) STS frameworks [Online handout]. Retrieved from UVA Collab: https://collab.its.virginia.edu/access/content/

Christin, N. (2012). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. *Carnegie Mellon INI/CyLab.* Retrieved from http://arxiv.org/pdf/1207.7139.pdf

Galvagna, C. (2019). The necessity of human rights legal protections in Mutual Legal Assistance Treaty reform. *Notre Dame Journal of International & Comparative Law*, 9(2) , Article 5. Retrieved from https://scholarship.law.nd.edu/ndjicl/vol9/iss2/5/

Gehl, R. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society*, *18*(7), 1219-1235.

Goldschlag, D., Reed, M., & Syverson, P. (1999). Onion routing for anonymous and private internet connections. *Communications of the ACM*, *42*(2), 39-41.

Jardine, E. (2015). The dark web dilemma: Tor, anonymity and online policing. *Global Commission on Internet Governance Paper Series*, 21.

Jardine, E. (2018). Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New media & society*, *20*(2), 435-452.

Jones, N., Arye, M., Cesareo, J., & Freedman, M. (2011). Hiding amongst the clouds: A proposal for cloud-based onion routing. *FOCI*. Retrieved from https://www.usenix.org/legacy/

Kalpathi, V. (2020). *A sociotechnical view of relationships between TOR users and national regimes*. [Figure 2]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Kalpathi, V. (2020). *The onion router in the context of Pacey's Triangle.* [Figure 3]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Khan, S. M., & Hamlen, K. W. (2012, June). AnonymousCloud: A data ownership privacy provider framework in cloud computing. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 170-176). IEEE. Retrieved from https://ieeexplore.ieee.org/stamp/

Laurikainen, R. (2010). Secure and anonymous communication in the cloud. *Aalto University School of Science and Technology—Department of Computer Science and Engineering, Tech. Rep. TKK-CSE-B10*, 1-5.

Mortier, R., Madhavapeddy, A., Hong, T., Murray, D., & Schwarzkopf, M. (2010). Using dust clouds to enhance anonymous communication. *Cambridge International Workshop on Security Protocols* (pp. 54-59). Springer, Berlin, Heidelberg.

Nastuła, A. (2020). Dilemmas related to the functioning and growth of Darknet and the Onion Router network. *Journal of Scientific Papers—Social development and Security, 10*(2), 3-10.

Nedeltcheva, G. N., Vila, E., & Marinova, M. (2019). The onion router: Is the onion network suitable for cloud technologies. *Smart Technologies and Innovation for a Sustainable Future* (pp. 389-398). Springer, Cham.

Omand, D. (2015). “The Dark Net: Policing the Internet’s Underworld.” *World Policy Journal*. Retrieved from http://worldpolicy.org/2015/12/09/the-dark-net-policing-the-internets-underworld/

Pacey, A. (1983). *The culture of technology*. MIT press.

Unger, N., Dechand, S., Bonneau, J., Fahl, S., Perl, H., Goldberg, I., & Smith, M. (2015). SoK: secure messaging. *2015 IEEE Symposium on Security and Privacy* (pp. 232-249). IEEE. Retrieved from https://ieeexplore.ieee.org/stamp/

Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism*, *39*(3), 195-206.

Woods, A. (2015). Data beyond borders: mutual legal assistance in the internet age. *Global Network Initiative*.