The Double-Edged Sword of the Dark Web: Its Implications for Medicine and Society

Hossein Akbarialiabad, MD[1], *Behnam Dalfardi, MD*[1], *and Bahar Bastani, MD*[2]

[1]Department of Internal Medicine, Shiraz University of Medical Sciences, Shiraz, Iran; [2]Division of Nephrology-Department of Medicine, School of Medicine, Saint Louis University, Saint Louis, MO, USA.

J Gen Intern Med 35(11):3346–7
DOI: 10.1007/s11606-020-05911-1

The interconnected network (Internet) can be imagined as an iceberg that has three layers: (1) the "surface web" that can be reached via conventional search engines like Google; (2) the "deep web" that is made of entities such as transactional databases and password-protected email accounts, which are supported by logins and are not indexed in search engines. These two layers can be reached via regular Internet browsers. The third layer is the "dark web" or "the dark side of deep web" that is only accessible by unique browsers, such as Tor ("The Onion Router"). Data and persons are anonymous in the dark web, where commerce takes place by cryptocurrencies, such as bitcoin, and cannot be traced easily by the governments. These two features make the dark web, a perfect place for illicit transactions, such as trade of private medical information, illicit drugs, and weapons (biological, nuclear, chemical, etc.), as well as organ trafficking and many other illegal activities. To make its magnitude clearer, in 2017, it was estimated that only 4% of the web was available on the surface web, and the remaining 96%, with 7.9 zettabytes, belonged to the dark web.[1] Below, we will briefly present some of the activities that occur in the dark web.

In recent years, transplantation tourism and modern slavery have become of great concern, globally. Transplantation is considered the best mode of treatment for patients with end-stage kidney disease. In 2018, the number of kidney transplantations in the USA was around 21,000; however, the number of transplant candidates in waiting list was around 100,000. Every year, around 10% of those on the wait list die or become too sick to be transplanted.[2] Not surprisingly, wealthy candidates will turn to alternative options. It is estimated that the crypto market covers 5 to 10% of kidney transplant market. With the spread of Internet technology from 2005 to 2013, the pattern of organ trafficking has changed from local to global. On darknet, the price of a transplantable organ doubled from 2008 to 2015 and now is around $40,000. Such transplants are associated with a high potential risk to both donors and recipients, since it demands a high level of patient care for both preoperative and postoperative management. Thus, it is the responsibility of all physicians who deal with transplant candidates to warn them of social media and dark web advertisements of organs, and their possible hazards.[3]

The trade of illicit drugs via the Internet dates back to a marijuana exchange between Stanford students and their counterparts at Massachusetts Institute of Technology (MIT) in 1971 or 1972 utilizing ARPANET (Advanced Research Projects Agency Network) accounts at their labs. With the expansion of Internet and social media, online drug trading has become more prevalent over time, the most memorable network being "Silk Road," which was seized by the FBI in 2013. The FBI announced that this website had a 1.2 billion-dollar turnover, with 80 million dollars in commission for administrators within 2 years of its establishment. Nowadays, there are crypto markets where a person can conveniently purchase anything illicit from benzodiazepines to cocaine, and that material can be delivered to almost any place worldwide via regular mail. Interestingly, consumers seem to be satisfied with purchases on the dark web. Crypto markets are equipped with potency ratings for drugs and a robust feedback system, so the purity of drugs and the accountability of vendors are surprisingly high. As a result, the risk of contamination, dilution with other products, or overdose has become less than street transactions. Also, due to anonymity, the risk of direct physical violence or harassment by drug-dealing gangs has diminished. Notably, there are many harm reduction forums found on the dark web, in which consumers share such information as to how to take a drug safely (i.e., optimal dosage, share personal experience of a drug, and even advise on how to quit a drug), basically in a non-judgmental "Narcotics Anonymous" forum. It has been suggested that medical personnel participate in/infiltrate such forums to provide the appropriate information in an anonymous fashion.[4]

Almost all online data/devices are susceptible to online attacks. In 2016, hackers stole medical records of nearly 16 million Americans from healthcare organizations. At that time, an individual's full medical records, including family history, were traded for around $20 to $50 on the dark web. It has also been shown that almost any electronic device, from a

Received March 3, 2020
Accepted May 4, 2020
Published online May 18, 2020

ventilator to an insulin pump, can be hacked. Imagine a case where you are a cardiologist, and somebody desires to kill your patients who use cardiac defibrillator. That person might easily do that by accessing the stolen medical records of the victims and hacking their devices. This should be of a great concern for us in the "Artificial Intelligence Millennium."

Healthcare providers and patients should be educated about such potential hazards. We must maximize patients' medical information/data security in the digital era. The electronic/digital banking of patients' medical information is at the beginning stage in many developing countries, and this should proceed only under full security. As more detailed personal medical data, such as whole-genome sequencing, becomes available for clinical decision making, more stringent security should be devised on protecting such personal medical information. In a worse-case scenario, it is imaginable that by hacking personal genomic data and designing biological agents (such as specific viruses), mass destruction could occur.[5]

Child sexual abuse is another instance of the negative impact of the dark web on community health. In many developed countries, children and pedophiles have easy access to the Internet, which has become a fertile ground for online sex offenders. This demands the attention of all families and medical practitioners, especially pediatricians and child psychiatrists.[6] Moreover, "red rooms" are online live rooms on the dark web where victims, especially women, are tortured and killed at the request of customers who pay in bitcoin. Also, terrorists predominantly use dark web to communicate with their members and propagate their ideologies, as well as providing instructions on how to make and/or activate weapons and warfare.

The dark web has some benefits too. Anonymity makes it a safe venue for whistleblowers to release reports about corruption in health governance and stewardship, drug approvals, as well as healthcare insurance companies that is not feasible by other means. Furthermore, for researchers in the Third World countries, where the research budget is so meager, access to scientific information, articles, and books from deep/dark web is a rescuer; however, the ethical implications should be addressed separately.

While the governments have attempted to block the dark web content over the past few years, dark web providers have introduced more user-friendly and secure tools, such as "Open Bazaar." In order to address this evolving phenomenon and to have a world free from illicit drugs and human abuse, a high level of international collaboration, such as a powerful and interdisciplinary expert committee of the WHO, Interpol (International Criminal Police), and other stakeholders, is required. We should understand that success cannot be easily achieved by the minor actions of individual governments. And finally, it cannot be overemphasized that data security should be considered as an absolute necessity before implementing any new technology.

Corresponding Author: *Bahar Bastani, MD; Division of Nephrology-Department of Medicine, School of Medicine, Saint Louis University, Saint Louis, MO, USA (e-mail: bahar.bastani@health.slu.edu).*

Compliance with Ethical Standards:

Conflict of Interest: *The authors declare that they do not have a conflict of interest.*

REFERENCES

1. **Alnabulsi H**, **Islam R**. Identification of Illegal Forum Activities Inside the Dark Net. in 2018 International Conference on Machine Learning and Data Engineering (iCMLDE). 2018. IEEE.
2. **Bastani B.** The present and future of transplant organ shortage: some potential remedies. J Nephrol. 2019; doi:https://doi.org/10.1007/s40620-019-00634-x.
3. **Fraser C.** An analysis of the emerging role of social media in human trafficking: Examples from labour and human organ trading. International Journal of Development Issues 2016;15(2):98–112.
4. **Buxton J**, **Bingham T**. The rise and challenge of dark net drug markets. Policy Brief. 2015;7:1-22. https://www.swansea.ac.uk/media/the-rise-and-challenge-of-dark-net-drug-markets.pdf
5. **Conaty-Buck S.** Cybersecurity and healthcare records. Am Nurse Today 2017;12(9): 62-64.
6. **Martellozzo E.** Policing online child sexual abuse-the British experience. European Journal of Policing Studies 2015; 3(1): 32-52.

Publisher's Note: *Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.*