

**THE RELATION BETWEEN INVESTIGATIVE JOURNALISM AND THE DARK WEB IN LEBANON:
IN LIGHT OF THE AUTHORITARIAN THEORY**

A Thesis

presented to

the Faculty of Humanities

at Notre Dame University-Louaize

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts in Media Studies: Advertising

by

ROLAND MOUNDALAK

May 2021

© **COPYRIGHT**

By

Roland Moundalak

2021

All Rights Reserved

Notre Dame University - Louaize
Faculty of Humanities
Department of Media Studies

We hereby approve the thesis of

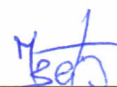
Roland Moundalak

Candidate for the degree of Master of Arts in Media Studies



Dr. Rita Sayyah

Supervisor



Dr. Maria Bou Zeid

Committee Member



Dr. Maria Bou Zeid



Acknowledgements

First and foremost, this research would have never reached this level of maturity and richness, were it not for the patience, understanding, guidance and commitment of an amazing professor: Dr. Rita Sayah. Huge respects to her, for never ever conveying any negative vibes whatsoever, but quite the opposite, her encouragement contributed largely to my motivation to keep going. This is how positivity breeds positivity, creating a ripple effect in a world where everything is interconnected. “When you learn, teach. When you get, give.” (Maya Angelou¹)

Much appreciation also goes to Dr. Maria Bou Zeid for dedicating her time to review this thesis, and for providing some important guidelines which resulted in a more refined end result.

And a huge thank you to the interviewees who agreed to share their valuable knowledge, with their referrals leading exponentially to even more interviews, thus forming a daisy chain* of inter-connected leads from different sectors (law, cyber-security*, military and media). Their participation has secured the progression through the already elusive topic that is the dark web*, let alone link it to investigative journalism in the Lebanese context.

¹ Maya Angelou (April 4, 1928 – May 28, 2014) was an American poet, memoirist, and civil rights activist.

Table of contents

Copyright	ii
Approval	iii
Acknowledgements	iv
List of Illustrations	vii
Abstract	x
Overview	xi
Introduction	1
Literature Review	3
Surface vs. Deep vs. Dark Web	3
Privacy: A legal and Ethical Perspective	4
Nature vs. Nurture	6
Stockholm Syndrome	7
For Want of a Nail	7
Investigative Journalism: A Brief Overview	8
The Dark Web	12
Cases That Involve Dark Web/Investigative Journalism	19
Theoretical Framework	28
Research Methodology	29
Research Questions	32
Data Collection and Analysis	33
Enter The Dark Web	33
Comparing Communication Technologies From A Privacy Perspective	37

Cyber-crime Law	38
Terrorism on The Dark Web	41
The Dark Web in Lebanon, by The Numbers	42
Hezbollah And Its Presumed Technical Capabilities	43
Lebanese Professional Research on The Dark Web	47
An Aborted Experiment	48
Aphorisms, And Some Unanswered Questions	50
Projections	51
Limitations	54
Conclusion	56
Glossary	58
References	71
Appendix A. Horror story: Who is Janice?	84
Appendix B. Deep Web (2015 documentary)	87
A True Story	87
The Production Team	90

List of Illustrations

This section contains statistical figures and charts, and it also assigns faces to the mentioned names in the upcoming stories.

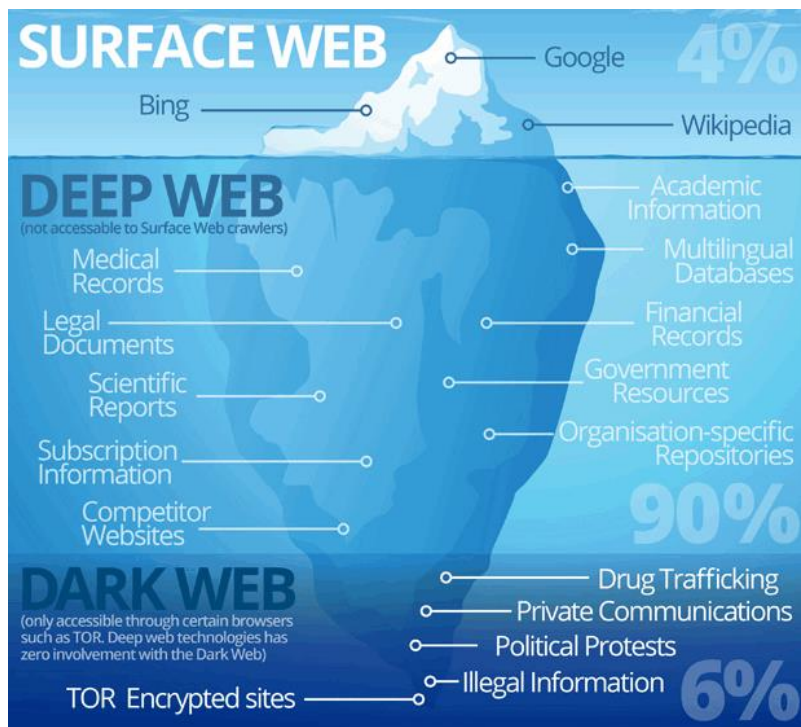


Figure 1



Figure 2 (<http://www.deepwebthemovie.com/>) (from left to right): Ross Ulbricht, Lyn (mother), Cally (sister), Kirk (father)



Figure 3 (<http://www.deepwebthemovie.com/>) (from left to right): Ross Ulbricht, Cally and Lyn and Ross, Ross Ulbricht



Figure 4



Figure 5



Figure 6

Requests	Percentage
Child Pornography	50%
Pornography Discussion	30%
Video Links	3%
Hidden Wiki Links	2%
Library Site Request	1%
Hacking Request	10%
Islamic Jihad Onion Link	1%
Money	1%
Questionnaire Link	1%
Government Documents	1%

Figure 7

The Anonymous Internet, 2015

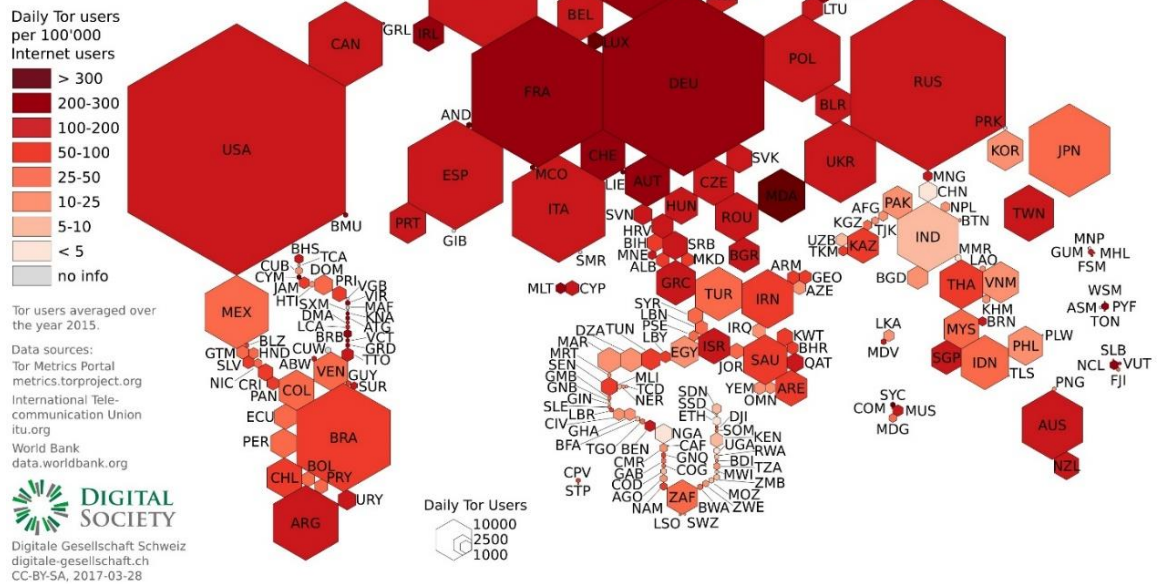


Figure 8

Abstract

For over 4 years (2017-2021), new content was constantly being added to this research, for a long-term observation of events, such as the rise and fall of Lebanese figures: after this paper's interviews, two of the interviewees witnessed their superiors being convicted (Khalil Sehnaoui from Krypton Security, and Suzanne Hajj Hobeiche from the Internal Security Forces).

The authoritarian theory was judged as most appropriate to convey the necessity of a technology that would allow private communication among citizens of oppressive regimes: most dangerously, however, is when journalists do not have the right to stand against their government; ironically, an authority only gives considerable freedom to minority thoughts and cultural issues to promote them if it doesn't make any threats to the authority.

Primary research was key in the search of genuine, unpublished results, which is essential for a topic of this specificity: interview questions were all about interlinking investigative journalism with dark web usage in Lebanon.

To summarize the findings, and among all the mentioned Lebanese internet cases that caught widespread attention, none was proved to have involved dark web usage (but none was proved otherwise, either); the private and public sectors in Lebanon both have the resources to undergo successful cyber-operations; until mid-2021, a cyber-crime* law was still not legislated*; dark web users in Lebanon make for less than 1% of all internet users; Al Jadeed investigative journalists are trained by a specialized organization (ARIJ).

Keywords: corruption, dark web, investigative journalism, Lebanon, mass communication.

Overview

An extensive glossary of 130 entries at the end of the paper aims at deciphering the jargon (technical or legal terms, mostly), so that readers of non-technical background can relate to the topic while potentially learning new terminology: included terms are marked with an asterisk

Introduction

"Someday we could be a shining beacon* of hope for the oppressed people of the world, just as so many oppressed and violated souls have found refuge here already. Will it happen overnight? No. Will it happen in our lifetime? I don't know. Is it worth fighting for until my last breath? Of course. Once you've seen what's possible, how can you do otherwise?" (Ulbricht, 2015) – full story included in appendix.

The dark web is the part of the world wide web [...] only accessible by [...] special software, allowing users [...] to remain anonymousⁱ, making a great tool for journalists and whistleblowers* to exchange “public good” related data secretly: when successful, this results in the mass distribution of the obtained information to the public, via various channels (i.e., TV, social media...).

While some studies suggest that the deep web* occupies 99% of all data on the internetⁱⁱ, others (figure 1) show that the deep web and its subcategory the dark web, account together to 96% of all internet data, and even the dark web alone ranks at 6%, which is 2% more than the surface web* and, just like an iceberg, the tip above the water is dwarfed by the massive volume underwater: of this 6%, one could enumerate drug trafficking, private communications, and more relevant to this paper, political protests and illegal information.

Speaking of political protests, one notable western example would be when Edward Snowden² used the dark web to leak information about the National Security Agency spying on US citizens: therefore, whistleblowing on such a national level can be considered as mass communication.

Building on the above, this paper aims to discover the role which the dark web plays in facilitating investigative journalism in Lebanon, and consequently, it aims to document the current practices and the role of the law in shaping social freedoms in the IoT (internet of things)* age during which privacy mutated from being the most basic right to become a privilege. To accomplish that, one-on-one interviews were conducted with professionals from media, legal and cybersecurity backgrounds, and from both the private and public sectors.

Before embarking on the topic, it is worth noting that the dark web is no different than other inventions, in being a tool that can fulfill a plethora of goals, depending on the intentions of the user: to put things into perspective, it is analyzed in this paper from a mass communication standpoint to unfold its impact in relation to the authoritarian mass communication theory which states that the media and press are only as free to express themselves as much as the governmental authorities allow them to be, and to add more controversy to the topic, the authoritarian theory is put to the test in Lebanon, a country which is known to be a democracy and (presumably) a fertile ground for free speech.

² Edward Joseph Snowden: American intelligence contractor and whistleblower who in 2013 revealed the existence of secret wide-ranging information-gathering programs conducted by the National Security Agency (NSA).

Literature Review

Drawing from a wide variety of scholarly materials, this study intends to define the dark web as a mass communication phenomenon, emphasizing audience, practice, and infrastructure as important factors to consider when determining its unique and abnormal status. The conditions surrounding the controversial existence of the dark web, particularly its original conception and subsequent creation as The Onion Routing project (Tor*), demonstrate the value of user information in the Digital Age – after all, knowledge is power (Stanley 2003). Thus, the dark web and other digital technologies permitting anonymous communication on the web can be considered as a form of protest through intervention, a means of rejecting the traditional mediascapes and embracing the alternative”ⁱⁱⁱ (Hargreaves et al., 2016).

Surface vs. Deep vs. Dark Web

1. Surface web (visible/indexed* web): it is the portion of the World Wide Web that is readily available to the general public and searchable with standard web search engines*^{iv}; it is made up of the social networks which everyone uses, the websites of their favorite brands, news sites, etc.
2. Deep web: it contains data which needs to be present on the internet for convenient access worldwide, by its owners and authorized personnel rather than by the public, such as academic research papers, bank account information, medical records, government-related classified information*, e-mail conversations: as a result, the deep web is the backbone of online lives.
3. Dark web: it falls under the deep web umbrella, but it requires special software and advanced technical skills to access, and its content ranges from free speech and anonymous

psychotherapy platforms to human trafficking, child pornography, and hitman hiring sites, so unlike what its name may suggest, it contains both good and ill-intentioned websites as this paper reveals. It is worth noting that the dark web was developed and is still funded by the US government^v, and it is where users can hide their identities and therefore render themselves (and the IP address* of their computer) untraceable by anyone, including law enforcement.

Privacy: A legal and Ethical Perspective

The word privacy is generally an ill-defined but widely understood term. A common correlation amongst the varied definitions is the availability, or lack thereof, of information on a given subject or individual whether they be primary or derived via analysis. In some countries, privacy is guaranteed by law or constitution*, such as human rights acts or bills concerning electronic data protection. In some cases, however, laws which guarantee privacy get superseded by more recent mandates* and edicts* passed down by higher echelons* like the EU parliament or global agreements like the Anti-Counterfeiting Trade Agreement. In this research, privacy is defined as the right of Internet users to not have their electronic data in any form analyzed or processed by any third party. This will include packet inspection*, traffic analysis*, and any means to discern the methods of privacy assurance such as cryptanalysis* or the defeat of tools used to provide privacy. As the current situation stands, there are a number of core problems facing privacy. These range from technical problems such as filtering* or traffic shaping* measures imposed by governments and “internet service providers”* to social problems such as a lack of awareness surrounding the subject of privacy^{vi} (Mc Manamon et al., 2010).

Looking at the bigger picture, the ethical and legal issues discussed here are distinct but related: ethics relate to the reasons why something is thought to be the right or wrong thing to do. Law relates to the rules a society has in place with which people can be coerced legitimately by the state into complying. Some ethical issues are reflected in the law; but ethics are broader than law: while illegal behavior is typically also unethical, much unethical behavior is not regulated by the law. Ethics is thus broader than the law, providing perspectives from which to criticize the law and argue for its reform. In practice, there is significant crossover between ethics and the law. For instance, “privacy by design”^{*} is an approach that began as best practice but is now being incorporated into EU Data Protection law. And ethics can have a key role to play in informing the law when, as is so often the case, the latter lags behind technological development. Technically, the content of the dark web is held within darknets^{*} which are privacy-sealed networks with the aim of hiding the IP address of the user and thus making their identity almost impossible to track and to uncover, and considering that “privacy-sealed networks” are achieved via software encryption^{*}, it is one reason why political dissidents^{*} and activists^{*}, journalists, law enforcement and the military benefit from using the dark web.^{vii} Some people, like Edward Snowden and Julian Assange³, see government-sponsored attempts to crack anonymity on the dark web as an attack on freedoms, especially privacy.^{viii}

³ Julian Paul Assange: Australian-born computer programmer and founder of WikiLeaks – an international, non-profit whistle-blowing organization that was created in Iceland in 2006.

Therefore, freedom in general, and freedom of speech in particular, is one of the main pillars of democracy, as it should be guaranteed for all citizens, including journalists since, ideally, the press has to be a major source of information for the people and the government alike, with the latter being required to stay as transparent as possible, and it is when it fails in this regard, that the role of journalism comes into play, by uncovering the mishaps committed by the ruling body: often described as the “fourth estate”^{*} due to the significant influence and lobbying power it holds, the press must remain out of the control of politics, in the legal as well as the financial sense.

Nature vs. Nurture

Just like freedom of speech is a pre-requisite to guarantee democracy, the former cannot be achieved without freedom of thought: one of the key distinctions between the Lebanese people and citizens in developed countries, is the way that some of the Lebanese perceive their political leaders as superhumans who never commit mistakes, but this mentality would not become ingrained within some sub-cultures if young generations were not inheriting it from their older counterparts: this debate involves the extent to which particular aspects of behavior are a product of either inherited (i.e., genetic) or acquired (i.e., learned) influences^{ix}: it is not an exaggeration to say that many educated Lebanese defend their political leaders and their quick enrichment by saying “this is their right, they want to continue to lead and this requires significant expenses”^o: such a perspective is the result of how citizens are nurtured, as opposed to the theory claiming that people are corrupted by nature: here comes the role of investigative journalism^{*} to shed light on illegal practices, and force the authorities on taking the appropriate measures which in turn lays the foundation for more aware citizens and more ethical politicians.

Stockholm Syndrome

Among the many factors that can hinder freedom of thought are psychological disorders, of which there became many after the Lebanese civil war, especially that many of its protagonists/antagonists never left the Lebanese political scene, which might explain the following theory: parliamentary elections are among the best ways to induce positive change in any democracy, yet the Lebanese keep on reproducing the same system that is drowning the country into corruption, and while some voters support specific candidates due to selfish and personal benefits (i.e. employment opportunities...), others are simply fearsome of the alternative which can unlikely be worse than a political system that “have thrust Lebanon into its worst economic crisis in decades”^x: this is defined as the feelings of trust or affection felt in many cases of kidnapping or hostage-taking by a victim towards a captor^{xi}: while some Lebanese are aware that the big leaders are carrying out major thefts, the tradition of political inheritance is still practiced at an alarming scale, on top of the Beirut blast, yet the people remain fragmented, unable to dethrone their sect leaders whose policies had brought the country down to its knees.

For Want of a Nail

To demonstrate the interdependence of the previously-mentioned concepts (freedom of thought – freedom of speech – democracy – psychological wellbeing), a multi-century old proverb goes like this:

“For want of a nail, the shoe was lost.

For want of a shoe, the horse was lost.

For want of a horse, the rider was lost.

For want of a rider, the battle was lost.

For want of a battle, the kingdom was lost,
And all for the want of a horseshoe nail.”^{xii}

Investigative Journalism: A Brief Overview

In a utopian society, there would be no need of investigative journalism, hence the role of the latter in increasing the redundancy of the system: in engineering, redundancy is the inclusion of extra components which are not strictly necessary to functioning, in case of failure in other components^{xiii}, so investigative journalism can be viewed as one of the last resorts for the public good in the fight against corruption, which is abundant in some countries: “In Lebanon investigative journalism has thrived after the eruption of the October 17, 2019 popular revolution against politicians that have robbed the people blind. News in the media has since been rife with reports on all forms of corruption. There are not enough investigative journalists to cover the vast cases of corruption in the country... And with the absence of accountability by the state, investigative journalists have taken it upon themselves to play the role of informant, investigator and police. They have pointed fingers at top officials, backed by damning reports and information”^{xiv} (Haddad, 2020). In Lebanon, the following examples suggest a potential for positive change, but only if the public opinion and the judiciary system were willing to reap the benefits of the hard work of an investigative journalist:

1. Beirut Port Blast: Investigative journalism in Lebanon has witnessed a rise in popularity especially after the Beirut port explosion on August 4th, 2020 which was one of the most devastating non-nuclear explosions in human history, to the point that it often spread more valuable information than the judiciary system did, both from a quantity and quality standpoint, despite bureaucracy* in public institutions and the difficulty of obtaining

official documents, especially that the influence exerted by politicians on the judiciary front is blocking any significant progress in the Beirut Blast case, for example, to the point that some international analyses about this incident were largely based not on official documents, but on photos and videos that were leaked by Lebanese journalists. As a result, by assuming the unfulfilled role of the judiciary system, the press becomes the biggest facilitator of transparent accountability towards a criminal and irresponsible political class which steals the money of its own people to build unjustifiable fortunes, only to pay a fraction of these fortunes to the same people during the elections to extend its presence.

2. Bold and responsible professionals: investigative journalism requires audacity, hence the importance of the journalist as the author of a message: people in developed nations did not obtain these freedoms except after a long struggle, confrontation and persistence. Investigative journalism is the gateway to a respectable press that, along with other institutions, contributes to supporting transparency and consolidating the concept of citizenship in a country where the politicians respect their electors, be it by sense of ethics or by fear of accountability. “It is the duty of investigative journalism, to address all kinds of topics that concern public interest, to inform the public and uncover their secrets. However, this general principle has exceptions, and the state may invoke the principle of relativism to interpret the legitimate interest and its right to intervene to prevent digging into certain topics that it considers, according to private or public data, as a matter that affects national security, public order, public safety, or public morals ...” (Sadaka et al., 2009).^{xv}

3. The Lebanese publications law (1962) and audio-visual law (1994) do not protect the journalists, but quite the opposite: criminal law classifies defamation* as a felony* and for

the most part, the truth that investigative journalists resort to is not used as a tool for defense. Besides, media laws do not allow journalists to view government documents, as they do not deny the matter, but they do not guarantee it either.^{xvi} At the same time, though, “the Lebanese judiciary system recognized the right for the journalist to publish their own information about the case despite the law’s prohibition of publishing the facts of the investigation and not the case itself that is being investigated. The press still has the right to publish what information it has, and even if publishing such information leads to an imbalance in the course of criminal justice, it remains imperative to maintain a balance between freedom of the press and its right to publish, and between the proper functioning of justice and the preservation of human dignity, as long as the prosecuted* person is not yet condemned or brought to trial. The discussed jurisprudence* is issued by the Court of Publications No. 127 dated 4-5-1972 and published in the Journal of Justice 1972 on page 396 published in its entirety in the appendices” (Sadaka et al., 2009).^{xvii}

4. ARIJ (Arab Reporters for Investigative Journalism) (<https://en.arij.net/>)

Being the first and leading media organization in the MENA region, dedicated to promoting investigative journalism across the Arab world, it was founded in 2005 with the aim of supporting independent, quality and professional journalism, by offering offline and online training, media coaching, mentoring, funding and networking opportunities with local and international media outlets.

The founder, Rana Sabbagh, is a career journalist since 1984, who devoted her time for almost 15 years in ARIJ to spread and consolidate the hitherto* unknown culture and practice of investigative journalism across Arab countries, starting in Jordan, Syria and Lebanon before expanding it into a Pan-Arab movement of “accountability journalism”.

As a proof of success in her field, she later moved to Sarajevo to work as MENA editor at OCCRP.ORG, a high-tech, non-profit global investigative journalism platform and network that specializes in cross-border crime and corruption, and which connects 45 non-profit investigative centers in 34 countries, scores of journalists and major regional news organizations across Africa, Asia, the MENA region and Latin America.

Traditional vs. Investigative Journalism:

Traditional journalism	Investigative journalism
Research	
Information is gathered and published / broadcasted at a steady pace (daily, weekly, monthly)	Information cannot be published unless it is complete and interconnected
The research is completed quickly, and gets discontinued after the story is released	Research may continue after the story is published / broadcasted
The story is based on a minimum of information, and can be very short	The story is based on the maximum information, and can be very long
Sources' statements can replace documentation	Requires field research and documentation to support statements
Relationship with the sources	
Trust in the source is assumed, and often without verification	The source cannot be assumed to be trusted, and information must be verified
Official sources provide information for free, to promote their goals	Information is hidden since exposing it may jeopardize the interests of the authorities
The journalist has no choice but to accept the story, although they could oppose it with comments or data from other sources	The journalist challenges the official narrative, and seeks information from independent sources
The journalist has less information than its individual sources	The journalist collects more information than its individual sources
Sources are often defined	Sources may be kept anonymous to guarantee their safety
Results	
The investigative report is seen as a reflection to the world who accepts it as is, and the journalist does not aim more than informing the audience	The journalist refuses to accept the world as it is, aiming to penetrate a certain situation to repair it, condemn it, or in certain cases, offer an alternative
The investigation does not require engagement and personal enthusiasm from the journalist	Without personal involvement and enthusiasm from the media, the story is never complete

The journalist seeks to be as objective as possible	The journalist seeks to be fair and scrutinized, even judgmental, based on their sources
The dramatic structure is not important, since the story has no end, and the news continue	The dramatic structure is essential to the impact which a story makes
The journalist may make mistakes, but they are inevitable and usually not very important	Mistakes have their repercussions on the journalist, and could endanger credibility

The Dark Web

While many people know about investigative journalism, this is not the case when it comes to the dark web: for instance, among the many people approached and asked if they know what it was, a tiny fraction responded positively, and none actually claimed that they ever used it, not because of its exclusivity since quite the opposite, almost anyone with a computer/phone/tablet and an internet connection can enter this digital underground with virtually no restrictions: in fact, most of those who refrain from accessing the dark web are held by the fear of getting caught using a mysterious technology that is associated more often than not with evil plans – hence the nomenclature “dark”.

And despite the fact that technology evolves over time, no matter what time period of history you look at there is always an underground of some sort – anarchists* and iconoclasts* who just don’t feel satisfied with what mainstream society offers; the only thing that’s really changed is the technology, and thanks to the internet, it’s possible to talk with like-minded people in anonymously and safely, anywhere in the world, and the free exchange of ideas can take place in its purest form; it sounds exciting and it really can be an experience like no other. However, curiosity killed the cat, as they say, so don’t divulge personal information on the dark web and think carefully about how you respond to

questions. After all, you don't know who the person on the other side of the conversation is, and participating in some of these communities can be rewarding and freeing, but like any adventure, you have to know and accept the risks before finally taking the plunge.^{xviii}

And those willing to take the risk might do it because they believe in the reward, whatever that might be... In his book titled "The Dark web: Inside the Digital Underworld", Jamie Bartlett was surprised in how much consumer-oriented markets on the dark web were, and continues to describe how developed the adult entertainment industry is, where a porn star can perform live shows that last up to 3 hours from their bedroom, to an audience that can tip by using bitcoin* currency (Bartlett, 2014)^{xix}.

"Even the faceless visitors to the dark web have a tendency to form interest groups and online communities with shared values. These aren't just sub-cultures, but sub-sub-cultures. Many of which would be socially unacceptable on the clearnet*^{xx}:

The Intel Exchange: people share information here that you would not normally expect, a lot of which is course pure fiction, conspiracy theories and the like, like Wikipedia but with less vetting*; even supposedly suppressed technologies get discussed here.

The Flashlight Forum: this is a dark web news service, which is a bit of a rarity, and where the visitor can read about what's going on in the dark web world with a fair amount of professionalism, albeit with a pinch of salt.

The Hub: this forum* hosts DoctorX, a real medical doctor who provides advice to drug users on the forum as part of The Hub's overall harm reduction practices, although it is an information exchange and strictly forbids buying and selling on the forum itself.

Anon Confessions: users anonymously write confessions, many of which are completely fictional, some of which are shockingly dark, but none of which is uninteresting; a rather

voyeuristic site, it showcases the sort of compulsion that makes people slow down when passing.

The Explosives and Weapons Forum: users interested in explosives or weapons come to learn and exchange information, and while simply knowing this stuff is not illegal in and of itself, it is about what the reader does with that knowledge.

Deep Web Ministries: Christian missionaries have been known to brave some of the darkest, most savage places on earth to spread their religious messages; on the dark web, their goal is to help people break free from vices such as narcotics* and illegal pornography.

Various Twitter Clones: in the real world of Twitter, you can get fired for a tweet or otherwise completely ruin your life, but the dark web twitter clones provide a place where you can speak your mind in public without repercussions – it is anonymous after all.

TorBook: Facebook already has an official dark web page, but ironically, the internet giant is all about making money from your personal info, so all this site does is allow you to securely access the real Facebook minus the personalized ads (read “minus the user’s exposed identity”).

Hacker Collectives: anyone who wants to join needs to be vouched for by a trusted member; alternatively, there might be some sort of vetting process; for a budding hacker this is where they will learn both the social structure of the hacking* community and the technical details of cyber-security; they can trust no one and at the same time, it really is a true human subculture; few are admitted, but by all accounts, this is where the most interesting stuff on the dark web happens, and what takes place here only makes it to the news later.

Places to avoid: while freedom of speech reigns supreme on the dark web, there are some communities that can get you in trouble simply for visiting them, so you should always use a VPN (virtual private network)* to hide the fact that you are using Tor from your ISP (internet service provider) and other nosy parties, but even so there is no reason to tempt fate; you should also consider the fact that some dark web pages may run scripts* that leave things on your computer that are traceable, which means using a virtual machine* might be a good idea. Apart from the technical and legal issues, you should also take into account the psychological toll some of the free-for-all image boards and forums can take: boards that deal with extreme violence, illegal adult sexual material, and other even stranger things can do real damage to your mental hygiene*; you are of course free to look at, read or watch whatever you like, but there is no such thing as media consumption without any consequences; if you happen upon such a place while exploring the deep web, perhaps consider backing out for your own safety and sanity.

Many renowned websites have an official dark web version such as:

Facebook: between June 2015 and April 2016, users of Facebook over Tor has increased from 525,000 to over 1 million people, and "This growth is a reflection of the choices that people make to use Facebook over Tor, and the value that it provides them".^{xxi}

WikiLeaks: dark web links are written in a different format than links from the "regular" web, and dark web links can also change periodically for the site to protect its privacy and security against hackers: for instance, the dark web equivalent of <https://wikileaks.org/>'s is <http://suw74isz7wqzpmgu.onion/>.

BBC: "The BBC has made its international news website available via the Tor network, in a bid to thwart censorship* attempts. The Tor browser* is a privacy-focused software used

to access the dark web. The browser can obscure who is using it and what data is being accessed, which can help people avoid government surveillance and censorship. Countries including China, Iran and Vietnam are among those who have tried to block access to the BBC News website or programs.”^{xxii}

6. The dark web in Lebanon: it is true that virtually anyone, anywhere can visit the above-mentioned sites, a quick internet search does not reveal any Lebanese or Arab-oriented similar site. And the scarcity of research papers on the topic in the Arab world in general, and in Lebanon in particular, does not help either, which was the main cause why this paper relies heavily on interviews and internet articles as information sources; so scarce, in fact, that even the few Arabic sites that talk about the subject, only mention American/European cases that took place in this cyber* underground, which makes one wonder if similar cases happened in the Arab world.

A Lebanese Army web article clearly states that ISIS resorted to the dark web as a means for mass communication with their audience: “Due to the dangerous role and function that ISIS plays on social media, Western governments, through their intelligence services, have attempted to prevent the organization from dominating the cyber public space, which led the takfiris* to search for new safe havens on the Internet, so the dark web was the perfect alternative, because it is not accessible, but a few users can browse it, because it is completely confidential. Experts consider that the informational messages sent and received on the Tor browser protect the identity of users through a complex process [...] so that they cannot be penetrated, and therefore cannot be tracked by any party. ISIS also provides digital guidance on how to use everything digital from social media to encrypted internet browsers such as Tor, and finally to saving emails”^{xxiii} (Mansour, 2017) : relating

this article extract to the main topic, an investigative reporter working through the Tor browser could monitor the activity of ISIS on the dark web, and even if the former did not necessarily manage to identify the identities of ISIS supporters, the obtained information could be partially and wisely deployed via mass communication means, with the goal of raising awareness within the global population to better shield their communities from such extremist mentalities. While cyber-security and intelligence firm Procysive estimates that the dark web is home to "more than 50,000 extremist websites and more than 300 terrorist forums"^{xxiv}, it can also be the place where political revolutions proliferate, so just like other technologies, the dark web can be a tool for both good and evil, depending on the intentions of the user.

Worth noting is that the scarcity (or absence) of published dark web cases in the country, might be due to the fact that such cases simply did not happen or, perhaps more suspiciously, because the Lebanese state is actively and purposefully preventing the publishing of such stories: if that is the case, one would wonder if the aim is to protect the citizens from each other, or to protect a corrupt political system from accountability.

In fact, Lebanon has always been regarded among the more open Arab countries regarding freedom of speech, despite a multitude of censorship cases and trials against activists and journalists, which can be an incentive for them to communicate via the dark web.

Bitcoin (the main currency used on the dark web)

After tackling the dark web market trends, markets would probably not exist in the first place without a way to organize payments, and here comes the role of Bitcoin, a currency that guarantees anonymity, making it an ideal match with the dark web: by definition, bitcoin is an uncontrollable asset, at least not by anyone other than its holder, because it

relies on a trustless system of payments, and “trustless” does not imply that the paying and receiving parties do not trust each other, but rather means that this new financial ecosystem along with its actors does not require a centralized entity, such as the case with traditional financial entities where the clients entrust a bank for example, on their money, in the hopes that their money would be safe and would remain their own.

Some of their qualities are anonymity and traceability: they are anonymous because the currency holder does not have to disclose their identity to anyone in order to pay or to get paid, but rather needs a “public key” which they use to receive money (to credit their digital wallet*), and a “private key” associated with the public key in order to pay someone else (thus debiting their digital wallet). This decentralized process enables the cryptocurrency* holder to remain anonymous, but there is a catch: since cryptocurrencies rely on a technology called blockchain*, the public keys are by definition public, thus prone to tracking, meaning that while no one necessarily knows to whom a bitcoin digital wallet belongs, but everyone can check at any time the history of a certain wallet, including the amounts that were ever deposited and withdrawn from it, as well as from which public key to which public key. It is worth mentioning that those keys are nothing but a string of code: for instance, 1JxCVTnk6s9hawcFSzNd1Uon7TQdcP21fQ is a public key, and 5K64uXtudqafXd2jxdpZRHvSVbZXFZxBGsnBwk1wFz6br2ghKZq is its associated private key.

While traceability is not a feature that would encourage a dark web user to trade by using bitcoin, the anonymity offered by this payment system is enough to lure traders, regardless of their underlying intentions.

Cases That Involve Dark Web/Investigative Journalism

1. The ARIJ / Al Jadeed TV partnership

The Hague case (better-known in Arabic as “محكمة العدل الدولية في لاهاي”), May 2015^{xxv}: a hearing was held in The Hague (Netherlands) in the context of the Karma Khayat / Al Jadeed being accused of “contempt of court”^{*} and “obstruction of justice”^{*}, and Rana Sabbagh was recalled as witness, claiming to have met on several occasions with the Al Jadeed team within the framework of ARIJ’s workshops, with one of the last training sessions that took place in 2010 being attended by Riad Kobaissi, “one of the best investigative journalists in the Arab world” as she describes him. When “prosecuting attorney”^{*} Kenn Scott asks Sabbagh “why do you think journalists in the Arab world need to improve their working methods?” in a clear allusion to the training sessions ARIJ is doing, she responds by evoking the multiple legal, political and social obstacles in the Middle East “which do not encourage investigative work”, emphasizing the risk of using the laws in this region to intimidate journalists. On several occasions, Ms. Sabbagh assures that in some cases, the journalist can override the laws and regulations in their practices and even take the risk of ending up in prison when his work is in the public interest. “This does not mean, however, that it must obscure the rules of ethics.”

2. The Ayman Jomaa case, June 2018^{xxvi}: Judge Carla Shawah of the Lebanese urgent appeals court rejected a request by businessman Ayman Jomaa to force retraction of a story about his businesses put out by Daraj, the Arab Reporters for Investigative Journalism (ARIJ) and Al-Jadeed TV. He wanted the story immediately removed, with each news outlet forced to pay a \$100,000 a day fine for every day they resisted. ARIJ said the story by Carole Kerbage and Eman Al-Qaisi in cooperation with the International Consortium of Investigative Journalists (ICIJ), was accurate and fair. “ARIJ never takes sides or goes after

any particular person or institution”, said ARIJ Executive Director Rana Sabbagh. “Our job is to look for evidence and to follow it to the truth, wherever that ends up.” The judge ruled that the request from Jomaa was “inconsistent with the principle of freedom of speech guaranteed in the Constitution” and she noted that the story was based on that is now available to more than 100 international media outlets, all partners of the ICIJ in the Panama Papers. The story Jomaa objected to focused on his considerable holdings in offshore companies and his failure to fully comply with questions and rules about ownership and capitalization of these firms.

3. The Suzanne Hajj Hobeich (figure 4) / Ziad Itani (figure 5) case

On November 23, 2017, Lebanese playwright Ziad Itani was arrested for being suspected as an accomplice with Israel^{xxvii}: shortly after his family confirmed his arrest, lawyer Joseph Abou Fadel claimed that Itani was planning with an Israeli officer to participate in the assassination of then-Lebanese Interior Minister Nouhad Machnouk as well as ex-minister Abd el Rahim Mourad^{xxviii}. Machnouk later announced on his Twitter account Itani's innocence, and the former even went on to apologize from the latter on behalf of the Lebanese people.

Afterwards, it was lieutenant colonel Suzanne el Hajj Hobeiche - then head of the Internal Security Forces cyber-crime and intellectual property* bureau - who was accused of fabricating the file to take revenge from Itani who, earlier during the same year, shared a screenshot showing her "liking" a tweet by Lebanese director Charbel Khalil, dated September 29 and which was deemed offensive to Saudi Arabia/Saudi women, thus getting Hajj Hobeiche fired.^{xxix} The case also involved Lebanese hacker Elie Ghabach who was reportedly employed by Hajj Hobeiche to fabricate the evidence that would implicate Itani

with the above-mentioned charges, and all three of them have successively served time in prison.

Needless to say, the case has captured nation-wide attention throughout the years, with involvement of major political parties, namely the Future Movement and the Free Patriotic Movement. Fast forward to almost 4 years after the initial arrest, Itani's lawyer, Diala Chehade, was expelled by force from the Military Court of Cassation* in the hearing session of Hajj Hobeiche and Ghabach, under the pretext of social distancing during the covid-19 pandemic: Chehade confirmed that this is a violation of the Lebanese law, so she filed a written complaint to the lawyers' syndicate Captain Melhem Khalaf, thus Atty. Chehade and her client, Itani, were both allowed to attend the next session.

Myriam Soueidan, a Lebanese journalist, published an article on April 4th, 2021, claiming the following: what is happening in the case of fabricating the file of Ziad Itani is a clear violation of Lebanese law and a perpetuation of the principle of not holding those with influence in Lebanon accountable: what really happened was the interrogation of the defendants* without the presence of anyone representing the other side, except that the Court of Cassation gave Hajj Hobeiche and Ghabach sufficient opportunity and space to change their statements in full view of everyone, especially after Ghabach was released from prison and he was able to coordinate with Hajj Hobeiche to change their story; this comes while Ziad Itani is absent, or rather, kept absent; Itani, who claims that he got tortured by officials when he was arrested, says "They are trying to silence me, but I will continue to talk ... I consider that the Lebanese state is my opponent with all its apparatus, but I will remain in the battle." And if the judicial authority has not yet tended to approve decisive and final rulings against everyone who participated in this complex crime, it was

a matter of morality and humanity for the political authority not to promote and congratulate the tormentor of Itani. However, this path does not seem surprising from an authority that is still, 8 months after the Beirut Port crime, unable to hold any perpetrators accountable, so that Itani's case appears to be a "marginal" file before an authority whose legitimacy has fallen.^{xxx} (Soueidan, 2021)

Months before the occurrence of the above scandal, an interview was conducted in 2017 with lieutenant Elie Dagher, then-subordinate of Suzanne Hajj Hobeiche. Also, Itani's lawyer, Atty. Diala Chehade, was interviewed in 2021.

4. The Khalil Sehnaoui⁴ (figure 6) case: just like Lt. Dagher was interviewed shortly before his superior Hajj Hobeiche was convicted, Eng. Jens Muecke was interviewed for this research a few months before his company's co-founder, Khalil Sehnaoui: "A man indicted* for hacking websites belonging to state-run telecoms company Ogero and Lebanese security institutions testified Tuesday before the Military Tribunal, claiming he deployed "secret programs" used by the U.S. National Security Agency to carry out his operation. Rami Saqr was arrested in July [2019], and in October [2019] was indicted for hacking and stealing confidential information about Lebanese General Security chief Abbas Ibrahim, as well as the names and cellphone numbers of senior security officers, their locations and their private telephone numbers. He was indicted along with two other suspects, including notorious hacker Khalil Sehnaoui, a partner at information security firm

⁴ A Belgian-Lebanese information security consultant who specializes in the Middle-East, and the founder and managing partner of Beirut-based Krypton Security; he is also a member of the Chaos Computer Club (CCC), Europe's largest association of hackers.

Krypton Security. Together the three men are accused of involvement in an even broader hacking operation that targeted Lebanese banks, government institutions and security agencies. He alleged that Sehnaoui had provided him with the secret programs used by the NSA to help him hack government websites. Once Saqr hacked the systems, he said, he would tell Sehnaoui, who would then inform the security agencies that their websites had been breached and offer them data protection”^{xxxix} (Diab, 2019).

5. Operation “Dark Caracal”: speaking of Krypton Security, and in light of the indictment of its co-founder Khalil Sehnaoui, Military Investigative Judge Riad Abu Ghayda said that “the act of piracy* [and hacking] has become one of the biggest challenges facing national security in all the countries around the world... Its danger is not limited to public institutions but also private companies, banks, residents’ freedom and money, intellectual property... It may seriously destroy the national economy”, and he adds that “the danger of hacking and piracy is holding this information ransom* and selling it for money”^{xxxix} (Diab, 2018).

According to new research from Lookout Security and the Electronic Frontier Foundation, “a string of spyware* campaigns operating out of a government building in Lebanon [the General Directorate of General Security building], dubbed “Dark Caracal” and linked to attacks on thousands of victims in more than 21 different countries, a range of targets so broad that researchers believe the campaign may represent a new kind of spyware for hire”^{xxxix} (Brandom, 2018). While the same article states that “It’s hard to believe Lebanon’s government is responsible for all of those campaigns”, if it actually proves to be true, it would indicate that the Lebanese state is very well established on the international hacking scene. Another article also states that “Cyber spies belonging to Lebanese General Directorate of General Security are behind a number of stealth hacking campaigns that in

the last six years, aimed to steal text messages, call logs, and files from journalists, military staff, corporations, and other targets in 21 countries worldwide. New nation-state actors continue to improve offensive cyber capabilities and almost any state-sponsored group is able to conduct widespread multi-platform cyber-espionage* campaigns. This discovery confirms that the barrier to entry in the cyber-warfare* arena has continued to decrease and new players are becoming even more dangerous^{xxxiv} (Paganini, 2018).

6. The case for using Tor in Arab countries: Arma, a blogger* on the Tor Project, one of the most popular dark web networks, narrates back in 2011: “Jake, Arturo, and I went to Tunisia Oct 3-7 to teach a bunch of bloggers from Arab countries about Tor and more generally about Internet security and privacy. The previous meetings were in Lebanon. On the keynote day, Jake and Arturo did a talk on mobile privacy, pointing out the wide variety of ways that the telephone network is "the best surveillance tool ever invented". The highlight for the day was when Moez Chakchouk, the head of the Tunisian Internet Agency, did a talk explicitly stating that Tunisia had been using Smartfilter since 2002, which is a content blocking software to target two categories of material: pornographic or sexually explicit sites, and anonymizer* sites that allow users to bypass the state's filtering. Syria and Israel seem to be the scariest adversaries in the area right now, in terms of oppression technology and willingness to use it. Or said another way, if you live in Syria or Palestine, you are especially screwed. We heard some really sad and disturbing stories; but those stories aren't mine to tell here. One of the points Jake kept hammering on throughout the week was if anything is being filtered, then you have to realize that they're surveilling everything in order to make those filtering decisions. The Syrian logs help to drive the point home but it seems like a lot of people haven't really internalized it yet. We still find

people thinking of Tor solely as an "anti-filter" tool and not considering the surveillance angle" (Arma, 2011)^{xxxv}.

7. Horror story: Who is Janice?^{xxxvi} Summary: this creepypasta* starts with Mark Spielman, an expert in the internet, who learns that the police department was looking for someone like him to hire: while surfing the dark web for child pornography sites, he discovered a suspicious site displaying the image of a girl, Janice, and after digging some more all of his computer files got deleted and replaced with photos depicting her, showing some disturbing facial expressions... The images finally morph into one with a man cutting the girl's stomach rip open along with her dead face. Afterwards, Mark Spielman went missing and the police discovered these findings on his computer. The full story can be found in the appendix, in the end of the paper. Reflection: whether the "Who is Janice?" story is real or pure fiction, it clearly demonstrates how extremely criminal the dark web can get, and how intertwined with real life it is.

8. Deep Web (2015 documentary) (<http://www.deepwebthemovie.com/>)^{xxxvii}^{xxxviii}^{xxxix}^{xl}^{xli}: this is one of the dark web's most controversial true and ongoing stories, in which some of those involved has attested "I'm not gonna be able to come to a conclusion about this": the documentary ends with the hero-criminal / evil-prosecutor dilemma as a window that remains wide open, to the thirst of the audience, rendering them confused about who is the protagonist and who is the antagonist. The story is about the rise and fall (or "the rise and rise", as some might argue) of Ross William Ulbricht and the history of Silk Road, a dark web site that supposedly allows all kinds of sales but has essentially become an online drug sales platform; Ulbricht was sentenced to a double life sentence, with his conviction based in part on the fact that he allegedly ordered several assassinations, charges which were

(more or less) dropped during the trial but which would have served to tarnish his reputation; it talks about bitcoins, internet freedom, invasion of privacy, all subjects that have occupied the newspapers lately and in which the American state still has a role; the documentary is obviously partisan, pretending to be careful not to draw conclusions, so from this point of view, it does not seem very honest and viewers may come out with the desire to watch more; the story is still pretty crazy; it was the anarcho-libertarian social network, and the rather handsome former boy scout character at the center of it all remains very mysterious; the archive footage at the end of the documentary is as striking as the movie itself. The movie's main character, Ross Ulbricht (figures 2 and 3) once said "The most widespread and systemic use of force is amongst institutions and governments, [and] the best way to change a government is to change the minds of the governed". By contrasting the keywords of the above, "audience" stands on the receiving end of an interaction, while "governed" means that there is an opportunity for change, making governance a two-way phenomenon where both "governed" and "governor" can have their input.

Theoretical Framework

Using the authoritarian media theory, the dark web is studied in an attempt to determine when authoritarians intervene in a communication process, and when this intervention transform into oppression: ethics is broader than law, hence it must define the legal context in a way that prevents activists in general, and investigative reporters in particular, from becoming outlaws.

“Mass media, though not under the direct control of the state, had to follow its bidding [...] Censorship of the press was justified on the ground that the state always took precedence over the right to freedom of expression on an individual level. This theory stemmed from the authoritarian philosophy of Plato (407 - 327 B.C), who thought that the state was safe only in the hands of a few wise men. [...] Engel, a German thinker further reinforced the theory by stating that freedom came into its supreme right only under authoritarianism*. The world has been a witness to authoritarian means of control over media by both dictatorial and democratic governments”^{xlii} (Suresh, 2003).

The authoritarian theory suggests that journalists “should not have any rights to comment, discriminate or stand against the government. Sometimes, an authority gives considerable freedom to minority thoughts and cultural issues to promote them if it doesn’t make any threats to the authority or ruler.”^{xliii} Therefore, the dark web fits well in the picture by being a refuge and a platform for expression at the same time, because not only does one have the ability to express themselves online, but they can do so in much broader limits and all while remaining anonymous.

Research Methodology

This research project mainly relies on qualitative research methods, precisely the interview technique, which not only yielded original and tailored results, but in this case, it has been imposed by the specificity of the topic: academic research about the dark web in Lebanon is already scarce – if existent – and this is even before narrowing the scope to include investigative journalism. Also dictated by the topic and the required outcome of this publication, qualitative data has been emphasized, for it is more relevant to find out the response of each interviewee to their profession-specific open-ended questions, than to limit the breadth of this untapped subject by collecting close-ended responses from a vast number of participants, the majority of whom might not have heard of the dark web.

To obtain the desired all-encompassing results, a selection of interviewees from the private and public sectors, and from diverse backgrounds, were interviewed to gather viewpoints on the topic under-study:

1. Atty. Charbel Kareh, attorney at law and PhD holder in information technology law, Master's degree holder in legal informatics*, and head of Internet Governance* Committee in Internet Society Lebanon Chapter, was asked about dark web activity in Lebanon, but his rather conservative answer was nevertheless indicative of the situation.
2. Atty. Diala Chehade: an expert on legislation in Lebanon, she is also the lawyer of Ziad Itani. During her interview, she tackled the subject of cyber-crime law in Lebanon.
3. Lt. Elie Dagher from the Lebanese ISF (Internal Security Forces) cyber-crime and intellectual property bureau, and the former subordinate of Hajj Hobeich. He shed lights on the efforts of their bureau to keep everything in check from a legal standpoint, since

regulating the cyber world has arguably become as important as the real world to keep national security in check.

4. Mrs. Elsy Moufarrej: content producer and audience coordinator at Sar El Wa2et in MTV Lebanon. She gave facts about the dark web / investigative journalism relation in Lebanon, she didn't hesitate to recall facts and names.

5. Eng. Gabriel Deek, general manager of OmniSystems SAL, and president and co-founder of Internet Society Lebanon Chapter. He gave insights on a controversial Lebanese party which also happens to be active outside Lebanese borders, whether through its armed forces or, possibly, via its cyber-warfare capabilities: Hezbollah.

6. Eng. Jean Saad: a cloud security* specialist at Cirrus. He talked about some real-life scenarios which took place in Lebanon, and some of which surprisingly suggest the offensive ability of the Lebanese state on the regional cyber-space* front.

7. Eng. Jens Muecke, senior partner and technical lead at Krypton Security: he explained how technology could be used to reveal the identity and address of a dark web user. Krypton is an advisory and consulting services firm, specialized in the domain of information technology and IT-related security.

8. Mr. Jimmy Ghazal (Notre Dame University alumnus), a media studies instructor at the American University of Beirut, and the innovation and digital director at M&C Saatchi, Mercury Content and Quantum Lebanon which is among the most respected Lebanese communications and media companies. Ghazal provided a general insight on the driving forces that might lead anyone to work in the dark web, especially as far as activists and journalists are concerned.

9. Dr. Joanna Baissary, head of Potech Labs⁵, and head of Potech Academy⁶: she narrated the experiment that Potech Labs conducted on the dark web, showing that her research scope stands well into dark web territory, where access to many forums is restricted.

In addition to the interviews, the dark web was accessed in an attempt to fetch information that is relevant to the topic: the particular process involved an unused smartphone, privacy-oriented software considerations, and a few hours of digging.

⁵ A Lebanese agency which “actively contributes to the issuance of research papers and various essential literature in the areas of cyber-security, as well as information & technology”

⁶ The privileged host of various workshops, conferences and other such training events, addressed to a wide audience of professionals as well as students in the field.

Research Questions

Q1: how does the barrier-to-entry for using the dark web prevent investigative journalists from obtaining valuable information?

Q2: what would a wide dark web adoption change in the mindset of potential users?

Q3: to which extent does admitting to using the dark web condemn the person?

Q4: who can prevent Lebanese public institutions from misusing the dark web?

Q5: how can the dark web promote free speech through journalism?

Data Collection and Analysis

This section is dedicated to stacking up new data to the ever-growing literature surrounding the dark web and investigative journalism in the region, by mashing up the interview answers in an attempt to shine a light on two sensitive topics which rarely – if ever – are mentioned together. At the same time, the information provided in the literature review is analyzed here, with the intention of building on what already exists as publicly-available stories.

Enter The Dark Web

This paper would be incomplete without actually accessing the dark web, in an attempt to find Lebanon-related journalism activity:

1. The process: find an unused Android device lying around → reset it → cover the cameras with paper tape → login to Play Store by using a specially-created Google account, and never use it afterwards → download “Tor Browser” and “Orbot: Tor for Android” → access the dark web → when finished, reset the Android device → uncover the cameras.
2. The findings: a couple hours of searching in the Tor browser show the massiveness of the alternative world contained therein: search engines (even Google has a fake version) are the probably the only way to navigate this realm, considering that the onion* links (the equivalent of the “www.xyz.com” website format) constantly change. Even a seasoned Google user might find it challenging at first to gain traction in the dark web search engines, because some try to omit potentially-illegal sites while others specialize in particular subjects. Keywords such as “Lebanon”, “journalism” and “politics” result in drug-related marketplaces*, Hezbollah and Syria news. With this, and the present whistleblower-

dedicated sites on tap, the potential is there, but some more digging is definitely required to find “valuable” data.

Discovering the above, and considering that an organization as important as ARIJ, holding a portfolio of numerous publications, does not mention the dark web as an integral part of investigative journalism, one might question if the Arab world in general, and Lebanon in particular, home to some highly tech-literate cultures, do not recognize the potential of the dark web, or if quite the opposite, the latter is proliferating while remaining a taboo subject that is omitted in discussions, just like other topics in the region, not the least of which is religion, sexuality...

Another curious thought, this time in the Hajj Hobeich / Itani case, revolves around computer wizardry, after hacker Elie Ghabach was presumably employed by Hajj Hobeich to potentially harm Ziad Itani, making it hard to imagine that a hacker of this caliber never used the dark web to accomplish his assigned task. Atty. Diala Chehade (Itani’s lawyer) was asked if she would learn a new technology such as the dark web, and she replied positively as long as that means that she would gain access to information and data which is unavailable on the traditional internet. She went on to say that from a legal perspective, one can use a technology that allows browsing the internet anonymously, as long as the user does not impersonate a public character or commit fraud.

The Hajj Hobeich / Itani case and the Sehnaoui scandal: potential dark web involvement: while these two stories were never proved to have involved dark web activity, Chehade is confident that among the Lebanese public institutions, at least the cyber-crime and intellectual property bureau uses the dark web, based on what took place during one of the interrogations in the Military Court. To complement her claims, a special talk with

cloud security specialist Eng. Jean Saad revealed his take on the matter: the IT veteran stated that while he is not in a position to confirm or deny what have actually happened, his technical knowledge makes him believe that obtaining the NSA-class hacking software used by Saqr and Sehnaoui have probably taken place on the dark web in the first place; in a similar fashion, any tech-savvy investigative reporter could resort to the dark web in order to obtain the hacking capability that enables her/him to infiltrate* into state-sponsored websites, with the ultimate goal of accessing (and spreading) corruption-related secret information. On a side note, while the two cases are unrelated, the Sehnaoui scandal happened with a private company, while the Hajj Hobeich / Itani case occurred with a public institution, and that is even more worrisome considering the regulatory role that the state must assume to guarantee fair and equal rights to all national stakeholders.

Atty. Kareh could not stress more that even if a dark web-related scandal happened in Lebanon, the most sensitive details would never surface in the media, and the same applies when a researcher approaches anyone knowledgeable in the matter, such kind of sensitive info do not, and usually should not, get disclosed to the public: interestingly, that is perhaps the most obvious reason as to why obtaining classified information for this research has been a challenging process, since the absence of evidence does not always negate events which have actually happened, but quite the opposite, it could imply the level of secrecy surrounding the dark web.

But being stealthy does not negate the sheer size of the deep web, with Lt. Dagher stating that approximately 7.9 zettabytes of the digital universe is on deep web sites

protected by passwords, in comparison to 0.33 zettabytes⁷ on the public web, which falls in line with the statement at the beginning of this paper that deep web data accounts to 96% of all internet data; this is why his team always keeps an eye on the deep web in general, and the dark web in particular, for national security purposes and by using methods such as ethical hacking* (also known as “white hat”*). He confirmed what Muecke said, and stated that in order to uncover a potentially malicious dark web user, his team goes through a trial-and-error process in order to mimic the expensive hardware/software which they cannot afford, a process that is not only much more time consuming and man-hour-intensive but also inefficient, because the aforementioned equipment that is available to much wealthier nations makes use of ultra-fast internet connections and supercomputers that the Internal Security Forces can only dream of: nevertheless, Dagher is vocal about what his division has achieved in keeping his country safe from the most threatening cyber-crimes. He also confirmed that the Internal Security Forces regularly organizes conferences about the dangers of the internet, yet it never raises the topic of the dark web, because any public talk about such an unknown topic would raise unwanted awareness that would result in a flood of newcomers, and once on the dark web, user identity becomes anyone’s guess, making the process more resource-intensive, from a human resource and financial perspective, for this law-enforcing agency to perform its duties.

⁷ One zettabyte is equal to 10^{21} bytes. One gigabyte is equal to 10^9 bytes. One megabyte is equal to 10^6 bytes.

If the above-mentioned interviews are of any indication, it would be that private and public institutions in Lebanon do not seem to lack any technical expertise to put themselves on the global espionage*/hacking scene, despite being less financially-capable than their counterparts from much larger countries, such as the USA, for example.

Comparing Communication Technologies From A Privacy Perspective

1. Dark web: since news organizations such as The Guardian use Tor to protect the privacy of political activists and whistleblowers, when asked what can the dark web add to the work of a journalist, investigator or even military professional, Lt. Dagher claimed that since the FBI themselves cannot technically “hack” the dark web (although they apparently did exactly that, as the Deep Web story goes, in the appendix), The Guardian and other organizations might fall victim to their actions if a dark web user ever decided to initiate a denial of service* attack on The Guardian website; Mr. Jimmy Ghazal pointed out that such agencies are the most susceptible to government censorship. Tor not only offers the advantage of end-to-end encryption, but also allows the user to hide their identity and location: if a Tor user wants to play it safe and make themselves even more untraceable, they could follow the below instructions:

- 1.1. Purchase a computer from a store which does not have surveillance cameras and which does not register the device serial number*.
- 1.2. Pay with cash, not a bank card, to avoid traceability.
- 1.3. Do not connect it to private networks such as their home or workplace Wi-Fi.

1.4. Rather than sending e-mails the traditional way, opt instead to save those e-mails in the draft folder where the intended recipient logs-in to the same e-mail address, and retrieve the content from that draft folder.

For better or worse, all these methods can be used by activists as well as by terrorists. And since legal prosecutions in Lebanon are based on goals and intentions regardless if the events are taking place on the internet or not, internet activity as the means of execution becomes nothing more than the evidence in a potential investigation; what is worth noting here, said Ghazal, is that the cyber-crime and intellectual property bureau has the duty of not becoming a tool for censorship but to stay focused on fighting crimes objectively and independently from political pressure.

2. SMS and “regular” phone calls: Ghazal also explained how people are suffering today from this censorship where, unlike some encryption-based online messaging services, SMS messages and non-internet-based phone calls are left "unprotected" from prying eyes and ears, and this is one additional reason why activists and the like avoid these traditional means of communication, and which is why high-profile individuals change their phone numbers regularly.

Cyber-crime Law

1. During the first half of 2017, Lt. Dagher claimed that there was no cyber-crime law in Lebanon, although one was being prepared: when legislated, and by being specific, such a law would make way for more fair verdicts in the case of violations: whenever deployed, this would enable officials to dissect each case: for example, if a sexual abuse scenario took place on Facebook, the investigators would deepen their analysis to take into consideration the nature of the profiles of the abuser and the abused, to find out if the threat came from a

personal profile, an official fan page, or a group... But in the case of arresting activists, does the dark web not become fertile ground for outlaws that are not necessarily "bad" people, one might ask? Dagher did not totally agree, claiming that the longest arresting time of activists is 2 days in general, and that is in a worst-case scenario when the President of the Republic himself was offended, but yes, those arrests do lead to more usage of Tor for example, which is not illegal (yet) in Lebanon, but regarded as very suspicious nevertheless. After all, the laws and policies that apply to the real life, apply to the internet as a medium as well, and when a crime or any offensive act takes place, the medium itself is not merely as important as the motives and results of the act. Ghazal, on the other hand, seemed more inclined to defend the activists, saying that since nowadays one cannot prevent a message from spreading, it either goes out openly, or it falls short of the knowledge of authorities who would not be able to identify the sender. In contradiction with what Dagher said, fast-forward almost 4 years after the interview, a cyber-crime law in Lebanon is still not legislated, and considering that the parliament has much more urgent matters to worry about in 2021 (financial crisis, covid-19...), it is hard to know if such a law would ever see the light: "following the previous support to the reinforcement of Lebanese legislation on cybercrime, a national workshop was organized on the 28th of October 2020, aiming to gather the Lebanese stakeholders responsible for drafting and enforcing the legislation on cybercrime and electronic evidence"^{xliv}.

Trying to understand what could be the reasons behind the delay (or abortion) of a cyber-crime law, Atty. Chehade responded on April 19th, 2021 that it was because the political parties simply did not reach an agreement over such a law, especially that the latter would give a legal formula for all existing news websites, which is not being completely fulfilled

by the current media law. She went on to generalize that when any law is being purposefully postponed, the underlying motive is that the political parties have not reached an agreement over it, either because it could benefit some of them while harming the others, or simply because it is not among their priorities.

2. An international insight: while the UK government, for instance, does not oppose using the dark web, to promote freedom of speech, China has established the so-called “Great Firewall” (in reference to the Great Wall of China) which imposes censorship and eventually pushes people to using the dark web.

3. Circumventing the law: Mr. Ghazal also had his say in this regard, saying that at its foundation, the internet was all about expressing and sharing, and censorship just ruins that, but while the UK and Europe in general do not practice censorship as much as China and other dictatorships, these very same governments also want to sniff* data, whether for elections or other purposes. In extreme cases such as in Syria where the internet was banned altogether, people at the borders with Lebanon were going online by using the Lebanese mobile network operators* MIC1 and MIC2, also known as Alfa and Touch. Ghazal also commented on the political decisions which occasionally result in arresting activists for their posts, which is dangerous, unless what is posted threatens public security, and talking about the ISF cyber-crime and intellectual property bureau, he went on to say that the team still wears a uniform and therefore cannot oppose the political decisions, which may in turn affect its performance and transparency.

4. The ISF fallacy: this state-backed office has its fair share of criticism: the bureau “extends its authority beyond the limits of the law by forcing detainees to sign a pledge not to repeat what they had written in a certain post, tweet, or comment or a pledge not to

malign a particular politician or cleric. The Bureau has also been known to force detainees to provide them with the password for a social media account and many more violations that contribute to the suppression of the right to freedom of expression^{xxlv} (Mahdi, 2019).

5. Breaking the law... By the cyber-crime and intellectual property bureau?! To be exact, it was the ex-head of this office – lieutenant colonel Suzanne Hajj Hobeiche – who was accused of hiring a hacker to wrongfully convict a presumably innocent person for illegally communicating with an agent from Israel, a country which is an official enemy to Lebanon.

6. Bitcoin-related law: Dagher affirmed that while bitcoin is not considered illegal, the upcoming cyber-law* should give it its legal nature, and he also revealed that almost all crimes that are encountered on the dark web are facilitated using bitcoin and other alternative cryptocurrencies – known by the umbrella term “altcoins”.

Terrorism on The Dark Web

1. Online recruitment: Ghazal admitted that the largest terrorist recruitment acts happen on the internet where organizations find ordinary people on social networks, and later communicate with them on special forums that may be on the dark web, and that is exactly what needs most to be surveilled by the authorities.

2. Fundraising assassinations: when Donald Trump was president of the United States of America, Crime Bay (a dark web site) hosted a bitcoin fundraising campaign aiming at assassinating him, which brings the question of how much of a new world order can be driven by a parallel world that is the dark web, and what chances do cryptocurrencies such as bitcoin stand, to go mainstream in the "real" world? According to Ghazal, it is possible, considering the untraceable nature of this currency, and legislations are still searching for ways to regulate bitcoin, but more work remains to be done on that front.

3. Online “sleeper cells”*: to Dagher, dark web communities can be sometimes compared to sleeper cells, since just like the Silk Road, an illegal dark web marketplace which was shut down several times, only to re-emerge online, these communities keep on coming back and resume operations until they eventually commit a technical mistake, revealing their identity to the ever-watching eyes of law enforcement.

The Dark Web in Lebanon, by The Numbers

1. Figure 7^{xlvi}: headed by Dr. Joanna Baissary, Potech Labs conducted a series of dark web chat room* investigations, discovering that, while child pornography-related talks occupied the top spot at 80% of all requests, the requests that could be linked to the topic - investigative journalism - only account to a mere 7% (the request total of video links, hidden wiki* links, library site request and, most importantly, government documents which is just 1%).

2. Figure 8^{xlvii}: according to this source, for every 100,000 internet users in Lebanon, there are up to 50 “Tor” users who access the dark web on a daily basis.

3. There were 5.35 million internet users in Lebanon as of January 2020^{xlviii}, considering a total population (mid-2020) of 6,825,445^{xlix}.

4. Summary: mashing the above data, a simple calculation and summary lead to the following:

4.1. Population = 6,825,445.

4.2. Internet users = 5.35 million = 78.38% of the population.

4.3. Daily Tor (dark web) users = 2675 = 0.05% of all internet users.

4.4. Daily Tor (dark web) users which could be linked to investigative journalism = 188 = 0.0035% of all internet users.

All dark web users are by definition minorities, with Ghazal believing that in Lebanon, they make for less than 1% of all internet users – not far from the above-calculated estimate – and their purposes vary widely, from naïve applications such as downloading pirated media, to threatening actions like terrorism. Religious, sexual or ethnic minorities are no different than anybody unless they are oppressed in a certain country, which in turn might push them to take refuge in the dark web.

Hezbollah And Its Presumed Technical Capabilities

Eng. Gabriel Deek suggested that Hezbollah, one of the more capable Lebanese political parties, might have an electronic army, which should not come to the surprise of anyone, according to him, considering its widely-known financial and technical prowess coming from Iran, which plays a crucial role in the warfare of Hezbollah with Israel (including cyber-warfare, for that matter): while it is challenging to confirm beyond a certain degree of certitude that Hezbollah does make use of the deep web (which includes the dark web), such statement is highly-unlikely to be wrong, given the abilities that it has in the south suburb of Beirut, also known as “Al Dahieh”. Arguably stronger than the Lebanese army^l, Hezbollah operates a digital facility that is “protected from electronic penetration* by exceptionally efficient firewalls* [...] strong enough to keep Israeli cyber experts from discovering the electronic center which dispatched the UAV [unmanned aerial vehicle*, also known as “drone”*] over their country and reaching its controllers.”^{li} Afterall, one cannot be top-of-game in warfare in the 21st century without having an intelligence division that complements their field capabilities: in reflection, these facts may be interpreted in a way which suggests that Hezbollah can theoretically “spy” on its local rivals (i.e. other Lebanese parties) to gain an “intelligence advantage” over them, which in turn affects the

public speeches of the “yellow party”, most of which are transmitted over the local news stations and as a result definitely fall under the mass communication category, and there is a good chance, judging from the above that the dark web can be, at least in theory, a key facilitator in this whole process.

Elsy Moufarrej, during a voice call on March 3rd, 2021, confirmed Deek’s claims by narrating a story which allegedly took place during the May 2008 Sunni/Shia conflict in Lebanon: after the Lebanese government declared the private telephone network of Hezbollah to be illegal^{lii}, street violence between Shia supporters of Hezbollah and Sunni backers of the Lebanese government intensified, noting that the Future Movement is the largest Lebanese Sunni political party, and this party runs a local television – Future TV: according to Moufarrej, Hezbollah individuals were sent to a Future TV caravan while the latter was covering the ongoing events, and used some hacking wizardry to disrupt the broadcasting signal of said caravan, which took the Future TV staff 5 days to resolve. Regardless of this story, Moufarrej admitted that freedom of expression nowadays has a much higher ceiling than the period when Syrian political presence in Lebanon was much more prominent; she also pointed out to some online resources that she considers as reliable sources, such as Daraj (<https://daraj.com/>), Megaphone (<https://megaphone.news/>), WikiLeaks (<https://wikileaks.org/>).

If Hezbollah – or any other political party – must have an investigative eye kept on them, then media outlets are in need of further training: Moufarrej reported that Al Jadeed

TV journalists have received investigative journalism training from ARIJ⁸ (a confirmed fact by ARIJ's founder herself^{fiii}), and she also mentioned the added cost of employing such type of projects: this type of reporting is especially resource-intensive, not just since it requires technical training, but also because investigations take more time to yield the desired results: any employer in the media should understand this, and allow their reporters to take the needed time to finalize a given case.

Of course, the needed time can be cut drastically in the event of massive online leaks: Moufarrej mentioned the Panama Papers as containing lots of important Lebanon-related leaks: these are 2.6TB of data or 11.5 million leaked documents that detail financial and attorney–client information for more than 214,488 offshore entities leaked beginning on 3 April 2016.^{livlvilvilviiiix} Most importantly, these leaks risk Lebanon into being listed on a list of uncooperative tax havens* that the Organisation for Economic Co-operation and Development (OECD) re-activated in July 2016 at the request of G20 nations, warned *Le Monde*, a French newspaper that participated in the investigation.^{lx} Also, *Al Akhbar* newspaper worked with WikiLeaks to fetch documents that might involve Lebanon, according to Moufarrej.

Drawing the similarities between the work of an attorney and an investigative journalist, Atty. Chehade declared that both have the duty to pursue the evidence and the perceptual document, especially in light of the legal basis available in conducting serious

⁸ Arab Reporters for Investigative Journalism: the first and leading media organization in the MENA region, dedicated to promoting investigative journalism across the Arab world.

and objective scientific investigations to reach the absolute truth: when a journalist discovers important information and shares it with the public, it is the duty of public prosecution offices to act upon receiving information about the occurrence of any crime, and to regard investigative media reports as news that they have the duty to investigate; and vice versa, when a lawyer discovers important information that may benefit the public interest, they become responsible to inform the state of any crime that they are aware of, and there is no legal barrier which may prevent the publication of information if it was to save lives, not endanger it; however, the catch is that the law punishes anyone who publishes information related to ongoing judicial investigations.

Speaking of legal work, Chehade was asked if her profession requires her to have a "self-sacrifice" attitude in order to put the public good first and foremost, and she responded that it is not a risk as much as it is to confidently and steadfastly adhere to the rights, duties and immunity of the legal profession or the press, and their original mission to reach the truth and achieve justice in the face of any security abuse, judicial repudiation*, or political targeting.

But not all members of the judicial system abide by the aforementioned rules, and the Joe Bejjani case is a clear proof as to how a news-shaking murder is followed by an arguably underwhelming legal reaction – or lack thereof: had it not been for the hand of treachery, one Monday morning in December 2020 was a normal day for Joe Bejjani, son of the town of Kahale located in southern Mount Lebanon, during which he took his children to school to complete his day of photography. The last thing Bejjani expected was two killers laying in the car park near his home, who had him killed with three shots from a pistol equipped with a silencer, only a few steps away from his children.^{lxi} One lesser-

known fact, as narrated by Moufarrej during her interview for this paper, is that when the killers took the phone of Bejjani and later threw it just 200 meters away from the crime scene, the police asked his wife to unlock the phone, and they discovered that, with some kind of hackery, the killers still had remote access to the smartphone, even though they possibly became tens of kilometers away: this revelation proves the technical capability that exists in a country that is small by area, but big with its never-ending problems.

Lebanese Professional Research on The Dark Web

Also on March 3rd, 2021, during a phone call with Dr. Baissary, she revealed that Potech Labs regularly use the dark web, and that they often find valuable information there:

1. According to her, nation-state actors also use the dark web for making plans, especially the likes of the USA and China, which falls in line with the claim in the paper introduction that the dark web is still funded by the US government^{lxii}.
2. Her organization established a dark web chat room for academic purposes, where they had to develop a chatbot* to reply to the other users to trick them into believing that they're dealing with someone from their community rather than with a cyber-security company: by employing this chatbot in tandem with their (Lebanese-made) software called "Darkivore", Potech Labs managed to obtain a plethora of results, not the least of which is figure 7, but since it is virtually impossible to reveal the locations of users on the dark web, figure 7 is not Lebanon-specific.
3. Dubbed as "The Cyberspace Hunter", Darkivore (<https://www.darkivore.com/>) assumes the following roles: identify exposed credentials, monitor digital footprints, prevent potential attacks, detect phishing*, create compliance reports, detect data leaked from corporations and exposed on the web, scrape deep and dark web onions, hunt leaked

information in the cyber-space, identify advanced threats, integrate threat sources, profile sellers.

4. Partnership with the Lebanese Army^{lxiii}: to further cement Dr. Baissary as a trusted source of information, her paper “Cyberattacks evolution” has received the Best Paper Award by the AISD (Artificial Intelligence for Security and Defense) in March 2019: AISD 2019 was a conference, organized by The Research and Strategic Studies Centre (RSSC) in the Lebanese Armed forces jointly with the “Lebanese Association for Information Systems” (LAIS) in Beirut, the “Middle East and North Africa Association for Information Systems” (MENA-AIS), and the “Information and Communication Technologies in Organizations” (ICTO) in Paris.

An Aborted Experiment

Taking inspiration from Potech’s dark web stunt, and with the goal of detecting any dark web activity that is related to investigative journalism in Lebanon, a proposed idea was to induce fake news as a bait, in one of the forums/marketplaces, but it was eventually deemed too risky for the researcher to undertake, especially after a string of executions post-Beirut blast (Joe Bejjani^{lxiv}, Lokman Slim^{lxv}...): the original plan was to post an advertisement on the dark web, which claims to include previously-unseen footage and evidence concerning the Beirut port explosion on August 4th, 2020. The challenges, however, are very real:

1. Danger ahead: the unregulated jungle that is the dark web is home to local and international players of political and/or criminal backgrounds who might be very interested in obtaining such footage, albeit for the wrong reasons.
2. Unindicative results: if the aim was to document the level of interest in such an advertisement, the most serious potential buyers of the photos/videos might be government

officials, political parties, journalists or anyone, really: it would be nearly impossible to determine who was the ultimate beneficiary of the aforementioned deal, yet alone figure out from which country the demand was coming.

3. Risk of getting caught: respecting the hardware and software requirements to surf the dark web anonymously does not guarantee that there are no vulnerabilities in the system which might allow a skilled hacker to figure out the real identity of the experiment performer. After all, there is no such thing as a flawless technology, as clearly demonstrated in the Silk Road story at the end of this paper.

4. An expensive adventure: some measures could be taken to achieve better levels of anonymity, but those do not come cheap. The ultimate cost, however, could be risking the researcher's life.

4.1. Avoid using one's personal computer: for traceability reasons, it is best to purchase a completely-new computer, in cash, from a store which does not have security cameras and which does not ask for the client's ID and phone number.

4.2. Ideally, the computer camera and microphone should be dismantled prior to turning it on.

4.3. The internet source, whether a SIM card or a regular router, must be purchased in the same fashion as the computer, privacy-wise.

4.4. The above hardware must be used solely for the experiment, before being destroyed: even donating it to someone might lead unwelcome visitors to their home, in a worst-case scenario.

Aphorisms*, And Some Unanswered Questions

1. The interviews that never were: the Pareto principle, also known as the 80/20 rule, states that for many outcomes, roughly 80% of consequences come from 20% of the causes (the “vital few”)^{lxvi}, and this could not be more true for the percentage of interview respondents in relation to the total of those who have been approached: for each 10 persons contacted, roughly 2 responded and answered their respective questions, which were tailored to every one of them, taking into consideration their professional background. But why did no single investigative journalist undertake the interview? Was it because of the topic? Or a simple coincidence? The list of approached (and reminded) reporters includes Adam Chamseddine, Edmond Sassine, Firas Hatoum, Jad Ghosn, Layal Bou Moussa, Layal Saad, Maroun Nassif, Riad Kobaissi, Riad Tawk and Salem Zahran. One of those replied with his phone number, but why did he change his mind when re-contacted later?
2. “Power tends to corrupt, and absolute power corrupts absolutely” (Acton⁹): if the dark web is not destined to evade authoritarianism, then what is it for? Is it a trap, set by none other than the US government, the initial developer and one of the current funders of the dark web?^{lxvii} And how tempting would it be for a developer to build a privacy-oriented technology, and resist leaving a backdoor (computing)?
3. No matter how deep one might dig into the dark web, does its “privacy by design” approach allow a researcher to reveal the location of data uploaders and downloaders? In a best-case scenario, where Lebanon-related files and stories are abundant in this internet

⁹ John Emerich Edward Dalberg-Acton, 1st Baron Acton, 13th Marquess of Groppoli, KCVO, DL (10 January 1834 – 19 June 1902), better known as Lord Acton, was an English Catholic historian, politician, and writer.

underground, there simply is no telling from which country these are being accessed. As a consequence, perhaps not all research papers are meant to reach a clear and absolute resolution, but is this not the essence of conducting a research in the first place, the possibility that the journey might lead to even more questions than those answered? Is the lack of satisfying evidence not a clear reminder of how mysterious some subjects can be?

Projections

Locally: as Lebanese public institutions continue to morph into digital-first entities, in opposition to the paperwork taking place, it is safe to assume that leaking government documents by an officer to a journalist would become a matter of a few clicks rather than having to carry thick paper files and risking getting caught: the dark web, in such case, can be the guarantee that both parties remain anonymous throughout the process.

Globally: there is no denial that the dark web is far from reaching even half its potential as an effective tool for injecting freedom of speech in today's "glocal"* societies, and only time can tell if this technology has the potential to become a necessity in the life of users, some of whom are growing more and more obsessed with their privacy.

To answer the research questions mentioned earlier, some of them were confirmed, while others were refuted:

1. The lengthy process to securely gain access to the dark web and the services it offers, can easily be a deal-breaker for anyone, especially less technology-oriented people, the most prominent of which older people.
2. While looking for the most suitable search engine to use, most were classified as yielding results about illegal websites, and illegal could range anywhere from drug marketplaces to media-rich crime sites; and in the case of child pornography sites, simply accessing them

would be illegal: therefore, potential users of the dark web could be very reluctant to enter this universe.

3. To claim that the dark web will ever take off as a mainstream technology is a mere prediction, and only time will tell if that will be the case: if so, then it could be caused by the subject becoming less of a taboo, and not the other way around.

4. The various uses of the dark web, as this these shows, are not limited to “dark” practices, but can also include online and anonymous psychotherapy sessions, and indeed, it really depends on what the user intends to do with this high-tech tool.

5. While someone might resort to the dark web because they have something to hide, this does not mean that they are guilty: for example, a whistleblower would like to contribute to social justice, yet at the same time without endangering themselves.

6. If someone took the necessary measures to surf the dark web securely, and their identity was still compromised, then this would underline a serious backdoor* in the technology itself.

7. News leaks exist everywhere, and even if it is nearly-impossible to catch a government-related entity “in flagrante delicto”*, there are always alternative ways to gather evidence, to prove that they actually resorted to the dark web for unfair play.

8. Just like drug dealers and their clients on the dark web are completely unknown to each other, the same relationship could exist between a whistleblower (selling the news) and an investigative journalist (buying the news).

9. The role of free speech is much more important when the audience is larger: so while the dark web promotes freedom of expression, it is yet to be seen if that would still be the case if more and more users came up: for example, whether the US government would

keep on funding the dark web^{lxviii} if more lobbies emerged in the future, or not, remains to be seen.

Limitations

“Time is a storm in which we are all lost.” (William Carlos Williams¹⁰): considering the breadth and depth of the topic, time was the most limiting factor in the development of the thesis, particularly when diving in the dark web: barely scratching the surface after a couple hours of using the Tor browser, the sheer amount of search engines on tap, indexing both legal and illegal sites, means that experience is not enough to navigate this labyrinth without falling on some sick-intentioned website, but even with the whistleblowing sites, timing is of the essence: for example, a news trading site allows anyone to post an article for sale, and as soon as the latter finds a buyer it gets removed, forcing a journalist to be attentive and patient to guarantee themselves a good catch.

As mentioned earlier, among all the professionals from various fields who were contacted for being interviewed, those that are most concerned with the topic – investigative journalists – had the lowest response rate: the most prominent reporters from the major Lebanese TV stations were all sent requests, but none undertook the interview. This leaves unanswered questions about the probable reasons of such a low response rate: in case the contacted reporters were too busy to answer, or were not knowledgeable about the dark web, this also applies to most of those who undertook the interviews, whether in-person or, post-coronavirus, via phone call or e-mail. And if the reporters do know/use the dark web, they may have felt threatened towards offering sensitive information to a stranger,

¹⁰ William Carlos Williams (September 17, 1883 – March 4, 1963) was an American poet, writer, and physician closely associated with modernism and imagism.

for publishing in an academic research, and during one of the most stressful political/economic times Lebanon has ever witnessed.

While Lt. Dagher and Mr. Ghazal were both authentic sources of information about the Dark Web practices in Lebanon and in general, with each one of them assuming the communications responsibilities of their respective institutions at the time of the interviews, their knowledge is not a match to the hands-on experience of a dark web user: for instance, it would be interesting to discover how they got in the game, and other things that only a dark web visitor has seen. But such an undertaking is on a whole new level since, the same logic that got those into the dark web in the first place, prevents them from even admitting that they ever accessed this digital underground.

Conclusion

In the end of this paper, one might wonder why at all would people use the dark web except for practicing illegal activities although strictly speaking, using it is not illegal, and as strange as it may seem, chatting and blogging on the dark web are actually being used by many investigative journalists and activists for the greatest of causes.

So, in reference to what Lt. Dagher said about not raising the dark web topic in his conferences, maybe the ones who need it the most would still find their way into this digital abyss anyway, and whomever is using it, for whichever intention, an essential goal from a user standpoint would be to never get caught.

One thing is for sure: while preparing this paper over the span of several years, asking acquaintances about people they knew who might have used the dark web, almost all of those approached did not have a clue what the technology was. Then again, investigative journalists might (and should) be an exception: known for occasionally trespassing the private properties of (presumably corrupt) politicians while on the lookout of the truth, it would be naive to assume they would omit the Pandora's box that is the dark web, from their repertoire. Perhaps they are too reluctant to use it, and maybe they do use it, but are simply hesitant to share this fact with strangers whose intentions are unknown, explaining why no single investigative journalist among the ten contacted persons, agreed to take the interview.

For better or worse, law enforcement in Lebanon is familiar with the dark web, as admitted by Lt. Dagher, and as confirmed by Atty. Chehade based on her findings during one of the interrogations in the Military Court. But whether the dark web played a pivotal role in the Hajj Hobeich / Itani case, remains (and might always be) a mystery.

There is no doubt that states and citizens have a reciprocating cat/mouse relationship, whereas law enforcement must stay on the lookout of potential breaches by the people who, in turn, have the fourth estate by their side, empowering them to lobby against any mistrustful government officials. And adaptability on both sides means that they can evolve to accommodate and learn new technologies to apply the law while also protecting free speech.

Nevertheless, justice remains fragile, not only within developing countries, but also in developed countries, as will be shown in the Silk Road case, where human rights got breached by the USA, one of the key promoters of human rights.

In all cases, the dark web could be thought of as the rawest and most real version of the internet, by being the quintessential replica of the tactile world in all its unregulated nature, and mirroring mankind's innate violence which, once social control ceases to exist, the law of the jungle is sure to swiftly fill the void.

Last but not least, this research proved one more time, that in the digital age, one genius and their computer can achieve outstanding results, thus circumventing the limited financials dilemma that a small country such as Lebanon might possess, hence the gravity of the "brain drain" that is affecting the country, now more than ever: losing brains in the 21st century is like robbing away immunity from a living organism.

Glossary

- _Activist: a person who campaigns to bring about political or social change.^{lxi}
- _Anarchist: a person who believes in or tries to bring about anarchy*.^{lxx}
- _Anarchy: a state of disorder due to absence or non-recognition of authority or other controlling systems.^{lxxi}
- _Anonymizer: a server that makes internet activity untraceable; it protects personally identifying information by hiding private information on the user's behalf.^{lxxii}
- _Aphorism: a short clever saying that is intended to express a general truth.^{lxxiii}
- _Appalling: extremely bad, especially from a moral point of view.^{lxxiv}
- _Authoritarianism: the enforcement or advocacy of strict obedience to authority at the expense of personal freedom.^{lxxv}
- _Backdoor (computing): a means to access a computer system or encrypted data that bypasses the system's customary security mechanisms.^{lxxvi}
- _Beacon: a source of light or inspiration.^{lxxvii}
- _Bitcoin: a type of digital currency in which a record of transactions is maintained and new units of currency are generated by the computational solution of mathematical problems, and which operates independently of a central bank.^{lxxviii}
- _Blockchain: a system in which a record of transactions made in bitcoin or another cryptocurrency are maintained across several computers that are linked in a peer-to-peer network.^{lxxix}
- _Blog: a regularly updated website or web page, typically one run by an individual or small group, that is written in an informal or conversational style.^{lxxx}
- _Browser (web): a piece of software used to view and interact with web pages.^{lxxxi}

_BSOD (blue screen of death): a screen that usually consists of an error message displayed in white text on a solid blue background and that occurs when an electronic device has encountered an error from which it cannot recover.^{lxxxii}

_Bureaucracy: a system of government in which most of the important decisions are taken by state officials rather than by elected representatives.^{lxxxiii}

_Censorship: the suppression or prohibition of any parts of books, films, news, etc. that are considered obscene, politically unacceptable, or a threat to security.^{lxxxiv}

_Chatbot: a computer program designed to simulate conversation with human users, especially over the internet.^{lxxxv}

_Chat room: a real-time online interactive discussion group.^{lxxxvi}

_Classified information: any data or material that belong to the federal government and relate to sensitive topics such as military plans or the vulnerabilities of security systems.^{lxxxvii}

_Clearnet: a term used by hidden web users to describe the regular internet.^{lxxxviii}

_Cloud computing: the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.^{lxxxix}

_Cloud security: the protection of data stored online via cloud computing* platforms from theft, leakage, and deletion.^{xc}

_Computer network: two or more computers that are connected with one another for the purpose of communicating data electronically.^{xcii}

_Constitution: a body of fundamental principles or established precedents according to which a state or other organization is acknowledged to be governed.^{xciii}

_Contempt of court: the disobedience of an order of a court.^{xciii}

_Creepypasta: internet horror stories or a myth passed around other sites, to frighten readers and viewers; the word, “creepypasta” comes from the term, “coppypasta”, an internet slang term for a block of text that gets copied and pasted from website to website.^{xciv}

_Cryptanalysis: the art or process of deciphering coded messages without being told the key.^{xcv}

_Cryptocurrency: a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.^{xcvi}

_Cyber: relating to or characteristic of the culture of computers, information technology, and virtual reality.^{xcvii}

_Cyber-crime: criminal activities carried out by means of computers or the internet.^{xcviii}

_Cyber-espionage: a form of cyber attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.^{xcix}

_Cyber-law: the area of law that deals with the internet's relationship to technological and electronic elements, including computers, software, hardware and information systems (IS).^c

_Cyber-security: the practice of protecting systems, networks, and programs from digital attacks.^{ci}

_Cyber-space: the notional environment in which communication over computer networks* occurs.^{cii}

_Cybercriminal: a person who engages in criminal activity by means of computers or the internet.^{ciii}

_Cyberwarfare: the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.^{civ}

_Cypherpunk: a person who uses encryption when accessing a computer network in order to ensure privacy, especially from government authorities.^{cv}

_Daisy chain: an interconnection of computer devices, peripherals, or network nodes in series, one after another; it is the computer equivalent of a series electrical circuit.^{cv1}

_Data mining: a process used by companies to turn raw data into useful information; by using software to look for patterns in large batches of data, businesses can learn more about their customers to develop more effective marketing strategies, increase sales and decrease costs; data mining* depends on effective data collection, warehousing, and computer processing.^{cvii}

_Dark web: the part of the world wide web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.^{cviii}

_Darknet: a computer network with restricted access that is used chiefly for illegal peer-to-peer file sharing.^{cix}

_Deep web: secret sections of the Internet whose contents are not accessible through standard search engines like Google, Yahoo, or Bing.^{cx}

_Defamation: the action of damaging the good reputation of someone.^{cx1}

_Defendant: a person who has been accused of breaking the law and is being tried in court.^{cxii}

_Denial of service (DoS) attack: an attack meant to shut down a machine or network, making it inaccessible to its intended users by flooding it with traffic.^{cxiii}

_Digital wallet: a software-based system that securely stores users' payment information and passwords for numerous payment methods and websites^{cxiv}.

_Dissident: a person who publicly disagrees with and criticizes their government.^{cxv}

_Drone: a remote-controlled pilotless aircraft or missile.^{cxvi}

_Eagle Scout: the highest rank of the Boy Scouts of America; a boy who has achieved this rank.^{cxvii}

_Eavesdropping: to listen secretly to what is said in private.^{cxviii}

_Echelon: a level or rank in an organization, a profession, or society.^{cxix}

_Edict: an official order or proclamation issued by a person in authority.^{cxx}

_Electronic penetration: a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security.^{cxxi}

_Encryption: the process of converting information or data into a code, especially to prevent unauthorized access.^{cxxii}

_Epiphany: a sudden, intuitive perception of or insight into the reality or essential meaning of something, usually initiated by some simple, homely, or commonplace occurrence or experience.^{cxxiii}

_Espionage: the practice of spying or of using spies, typically by governments to obtain political and military information.^{cxxiv}

_Ethical hacking: an act of intruding/penetrating into system or networks to find out threats, vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages [...] to improve the security of the network or systems by fixing the vulnerabilities found during testing.^{cxxv}

_Exculpatory evidence: evidence, such as a statement, tending to excuse, justify, or absolve the alleged fault or guilt of a defendant.^{cxxvi}

_Felony: serious crime that can be punished by one or more years in prison.^{cxxvii}

_Filtering (traffic): traffic filtering and application filtering (traffic filtering by Layer 7 application) are features that directly help get more visibility and security from less monitoring and security tools capacity; [the] purpose of traffic filtering [is] seeing more with less, securing more with less.^{cxxviii}

_Firewall: a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.^{cxxix}

_Flounder: to experience great difficulties or be completely unable to decide what to do or say next.^{cxxx}

_Forum: a meeting or medium where ideas and views on a particular issue can be exchanged.^{cxxxi}

_Fourth estate: the press; the profession of journalism.^{cxxxii}

_Glocal: reflecting or characterized by both local and global considerations.^{cxxxiii}

_Hacking: the gaining of unauthorized access to data in a system or computer.^{cxxxiv}

_Hacktivist: a person who gains unauthorized access to computer files or networks in order to further social or political ends.^{cxxxv}

_Hitherto: until now or until a particular time.^{cxxxvi}

_Iconoclast: a person who attacks or criticizes cherished beliefs or institutions; a destroyer of images used in religious worship.^{cxxxvii}

_In flagrante delicto: while committing the offence.^{cxxxviii}

_Indexing (web): the process by which search engines organize information before a search to enable super-fast responses to queries.^{cxxxix}

_Indict: formally accuse of or charge with a crime.^{cxl}

_Infiltrate: enter or gain access to (an organization, place, etc.) surreptitiously and gradually, especially in order to acquire secret information.^{cxli}

_Informatics: the science of processing data for storage and retrieval; information science.^{cxlii}

_Intellectual property: any product of the human intellect that the law protects from unauthorized use by others; the ownership of intellectual property inherently creates a limited monopoly in the protected property; intellectual property is traditionally comprised of four categories: patent, copyright, trademark, and trade secrets.^{cxliii}

_Internet domain: a unique name of an organization or person on the internet. For example, computerlanguage.com is the domain name for the publisher of this encyclopedia.^{cxliv}

_Internet governance: the rules, policies, standards and practices that coordinate and shape global cyberspace.^{cxlv}

_Internet of things "IoT": in the broadest sense, the term IoT encompasses everything connected to the internet, but it is increasingly being used to define objects that "talk" to each other. "Simply, the Internet of Things is made up of devices – from simple sensors to smartphones and wearables – connected together."^{cxlvi}

_Internet Service Provider "ISP": a company that provides Internet connections and services to individuals and organizations.^{cxlvii}

_Investigative journalism: the unveiling of matters that are concealed either deliberately by someone in a position of power, or accidentally, behind a chaotic mass of facts and

circumstances - and the analysis and exposure of all relevant facts to the public; in this way investigative journalism crucially contributes to freedom of expression and media development.^{cxlviii}

_IP address: a unique string of numbers separated by full stops that identifies each computer using the Internet Protocol to communicate over a network.^{cxlix}

_Jurisprudence: the science or philosophy of law.^{cl}

_Kingpin: the chief person in a group or undertaking.^{cli}

_Legal informatics: the academic field that concerns itself with the problematics of computers and law.^{clii}

_Legislate: make or enact laws.^{cliii}

_Libertarianism: a political philosophy that takes individual liberty to be the primary political value; it may be understood as a form of liberalism, the political philosophy associated with the English philosophers John Locke and John Stuart Mill, the Scottish economist Adam Smith, and the American statesman Thomas Jefferson; liberalism seeks to define and justify the legitimate powers of government in terms of certain natural or God-given individual rights.^{cliv}

_Mandate: an official order or commission to do something.^{clv}

_Marketplace: the arena of commercial dealings.^{clvi}

_Mental hygiene: the science of maintaining mental health and preventing the development of psychosis, neurosis, or other mental disorders.^{clvii}

_Military court of cassation: the permanent military tribunal (a trial court, known also as the PMC) and the military court of cassation are composed of a combination of military and civilian judges, the latter emanating from Lebanon's ordinary court system.^{clviii}

_Mobile network operator: a telecommunications service provider organization that provides wireless voice and data communication for its subscribed mobile users.^{clix}

_Narcotic: an addictive drug affecting mood or behavior, especially an illegal one.^{clix}

_Obstruction of justice: an act that "corruptly or by threats or force, or by any threatening letter or communication, influences, obstructs, or impedes, or endeavors to influence, obstruct, or impede, the due administration of justice."^{clxi}

_Onion (domain): a top-level internet domain* used by anonymous websites on the dark web. Access to onion sites is via the Tor browser.^{clxii}

_Outdoorsman: one who spends much time in the outdoors or in outdoor activities.^{clxiii}

_Packet inspection: a type of data processing that looks in detail at the contents of the data being sent, and re-routes it accordingly; it can be used for perfectly innocuous reasons, like making sure that a feed of data is supplying content in the right format, or is free of viruses; or it can be used for more nefarious motives, like eavesdropping* and censorship.^{clxiv}

_Phishing: a method of trying to gather personal information using deceptive e-mails and websites.^{clxv}

_Piracy (media): the unauthorized use or reproduction of another's work.^{clxvi}

_Privacy by design: an approach to systems engineering that seeks to ensure protection for the privacy of individuals by integrating considerations of privacy issues from the very beginning of the development of products, services, business practices, and physical infrastructures.^{clxvii}

_Prosecute: institute or conduct legal proceedings against (a person or organization).^{clxviii}

_Prosecuting attorney: an attorney who conducts proceedings in a court on behalf of the government.^{clxix}

_Ransom: a sum of money demanded or paid for the release of a captive.^{clxx}

_Repudiation: denial of the existence of a contract and/or refusal to perform a contract obligation.^{clxxi}

_Script: a computer script is a list of commands that are executed by a certain program or scripting engine; scripts may be used to automate processes on a local computer or to generate web pages on the web.^{clxxii}

_Search engine: a program that searches for and identifies items in a database that correspond to keywords or characters specified by the user, used especially for finding particular sites on the world wide web.^{clxxiii}

_Serial number: an identification number showing the position of a printed or manufactured item in a series.^{clxxiv}

_Sleeper cell: a terrorist cell whose members work under cover in an area until sent into action^{clxxv}

_Sniffing (data): theft or interception of data by capturing the network traffic using a sniffer (an application aimed at capturing network packets).^{clxxvi}

_Spyware: software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.^{clxxvii}

_Surface web: content on the world wide web that is available to the general public; the surface web is indexed by the major search engines.^{clxxviii}

_Takfiri: a Muslim who declares another Muslim to be apostate (i.e., not believing in the essential tenets of Islam) and therefore no longer a Muslim.^{clxxix}

_Tax haven: an offshore country that offers foreign individuals and businesses little or no tax liability in a politically and economically static environment.^{clxxx}

_Testify: give evidence as a witness in a law court.^{clxxxix}

_Tor (short for 'The Onion Router): an open-source privacy network that permits users to browse the web anonymously; Tor was initially developed and solely used by the US Navy to censor government communications before the network was made available to the public.^{clxxxix}

_Traffic analysis: the process of recording, reviewing and analyzing network traffic for the purpose of performance, security and/or general network operations and management.^{clxxxix}

_Traffic shaping: a congestion management method that regulates network data transfer by delaying the flow of less important or less desired packets; it is used to optimize network performance by prioritizing certain traffic flows and ensuring the traffic rate doesn't exceed the bandwidth limit.^{clxxxix}

_Travesty: something that does not have the qualities or values that it should have, and as a result is often considered wrong or offensive.^{clxxxix}

_Uncanny: strange or mysterious, especially in an unsettling way.^{clxxxix}

_Unmanned aerial vehicle "UAV": an aircraft piloted by remote control or onboard computers.^{clxxxix}

_URL: a uniform resource locator (URL), otherwise known as a universal resource locator, is the address of a resource on the internet and the protocol used to access it; it indicates the location of a web resource like a street address indicates where a person lives physically; because of this, an URL is often referred to as "web address".^{clxxxix}

_User interface: the means by which the user and a computer system interact, in particular the use of input devices and software.^{clxxxix}

_Vetting: investigating (someone) thoroughly, especially in order to ensure that they are suitable for a job requiring secrecy, loyalty, or trustworthiness.^{cxc}

_Virtual machine: a software computer that, like a physical computer, runs an operating system and applications.^{cxc}

_Virtual Private Network “VPN”: an encrypted connection over the internet from a device to a network; the encrypted connection helps ensure that sensitive data is safely transmitted; it prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.^{cxc}

_Warrant: a document issued by a legal or government official authorizing the police or another body to make an arrest, search premises, or carry out some other action relating to the administration of justice.^{cxc}

_Web browser: an application used to access and view websites.^{cxc}

_Web interface: a user interface* that is implemented in the form of a web page and can be navigated using a standard web browser.^{cxc}

_Whistleblower: one who reveals something covert or who informs against another.^{cxc}

_White hat: a person who hacks into a computer network in order to test or evaluate its security systems.^{cxc}

_Wiki: a website or database developed collaboratively by a community of users, allowing any user to add and edit content.^{cxc}

References

Lexico Dictionaries. (n.d.). Dark web. In Lexico.com dictionary. Retrieved May 13, 2021, from https://www.lexico.com/en/definition/dark_web

(n.d.). The Deep Web is the 99% of the Internet You Can't Google. Curiosity. <https://curiosity.com/topics/the-deep-web-is-the-99-of-the-internet-you-cant-google-curiosity/>

Hargreaves. (2017). Into the Abyss: The Darknet. Course Hero. <https://www.coursehero.com/file/pigovn/conflate-the-darknet-and-the-dark-web-with-criminal-behaviour-a-negative/>

Barratt, Monica (2015). A Discussion About Dark Net Terminology. Monica Barratt. <https://monicabarratt.net/a-discussion-about-dark-net-terminology/>

BBC. (2019). BBC News launches 'dark web' Tor mirror. BBC. <https://www.bbc.com/news/technology-50150981>

Waldo, J. & Lin, H.S. & Millett, L.I. & Council, National. (2007). Engaging privacy and information technology in a digital age. Research Gate. https://www.researchgate.net/publication/309109045_Engaging_privacy_and_information_technology_in_a_digital_age

University of Warwick. (2017). Policing the Dark Web: Ethical and Legal Issues. European Commission. <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c2573eef&appId=PPGMS>

Kushner, D. (2018). The Darknet: the Battle for 'the Wild West of the Internet'. Rolling Stone. <http://www.rollingstone.com/politics/news/the-battle-for-the-dark-net-20151022>

McLeod, S. (n.d.). Nature vs. Nurture in Psychology. Simply Psychology. <https://www.simplypsychology.org/naturevsnurture.html>

Hubbard, B. (2020). Lebanon's Economic Crisis Explodes, Threatening Decades of Prosperity. The New York Times. <https://www.nytimes.com/2020/05/10/world/middleeast/lebanon-economic-crisis.html>

Lexico Dictionaries. (n.d.). Stockholm syndrome. In Lexico.com dictionary. Retrieved May 13, 2021, from https://www.lexico.com/definition/stockholm_syndrome

Williamson. (2008). Citadel. "A Little Neglect May Breed Great Mischief". <http://www.citadel.edu/root/images/commandant/assistant-commandant-leadership/for-the-want-of-a-nail.pdf>

Lexico Dictionaries. (n.d.). Redundancy. In Lexico.com dictionary. Retrieved May 28, 2021, from <https://www.lexico.com/definition/redundancy>

Haddad, B. – V. (2020). Investigative Journalism Thrives in Lebanese Media, Remains Missing at Universities. Aawsat. <https://english.aawsat.com/home/article/2373276/investigative-journalism-thrives-lebanese-media-remains-missing-universities>

Sadaka, G., Karam, J., Rammal, A., & Mikhael, T. (2009). محاذير قانونية عامة. In 1376619778 1005979401 M. Chreim (Ed.), التحقيق الاستقصائي - مبادئ وتطبيقات (pp. 55-56). Beirut.

Dabbous, Y. (2012). تدريس الصحافة الاستقصائية في الدول العربية. UNESCO. <http://www.unesco.org/new/fileadmin/MULTIMEDIA/FIELD/Beirut/images/2.pdf>

Sadaka, G., Karam, J., Rammal, A., & Mikhael, T. (2009). محاذير قانونية عامة. In 1376619778 1005979401 M. Chreim (Ed.), التحقيق الاستقصائي - مبادئ وتطبيقات (pp. 55-56). Beirut.

Deepwebadmin. (2018). These Are Some of the Most Interesting Deep Web Communities. Deep Web Sites. <https://www.deepweb-sites.com/most-interesting-deep-web-communities/>

Bartlett, Jamie (2014). The Darknet: Inside the Digital Underworld.

Deepwebadmin. (2018). These Are Some of the Most Interesting Deep Web Communities. Deep Web Sites. <https://www.deepweb-sites.com/most-interesting-deep-web-communities/>

Facebook over Tor. (2021). 1 Million People use Facebook over Tor. Facebook. Retrieved May 13, 2021, from <https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624066877648/>

BBC. (2019). BBC News launches 'dark web' Tor mirror. BBC. <https://www.bbc.com/news/technology-50150981>

إعلام-داعش-الوسائل-والخطاب-الدعائي-والتقنيات. (2017). Lebanese Army. <https://www.lebarmy.gov.lb/ar/content/إعلام-داعش-الوسائل-والخطاب-الدعائي-والتقنيات>

McCormick, Ty (2013). The darknet.

OLJ. (2015). Affaire al-Jadeed : la directrice de l'association Arij invitée par la défense à témoigner. L'Orient-Le Jour. <https://www.lorientlejour.com/article/924730/affaire-al-jadeed-la-directrice-de-lassociation-arj-invitee-par-la-defense-a-temoigner.html>

COURT RULES IN FAVOR OF NEWS. (2018). Arab Reporters for Investigative Journalism (ARIJ). <https://en.arj.net/news/court-rules-in-favor-of-news/>

إخلاء-سبيل-المقدم-. Al Jaras. <https://aljaras.com/إخلاء-سبيل-المقدم-> /سوزان-الحاج-بشروط

زياد-عيتاني-. Al Jaras. <https://aljaras.com/زياد-عيتاني-> /يعترف-بالعمالة-والتخطيط-لإغتيال-نهاد

إخلاء-سبيل-المقدم-. Al Jaras. <https://aljaras.com/إخلاء-سبيل-المقدم-> /سوزان-الحاج-بشروط

Soueidan. (2021). قضية زياد عيتاني: السلطة تعبت بالقضاء مجدداً. Daraj. <https://daraj.com/69480/>

Star, Y. D. T. D. (2019). 'Secret' programs used by NSA deployed in Lebanon hack: accused. The Daily Star. <http://www.dailystar.com.lb/News/Lebanon-News/2019/Mar-20/479285-sehnaoui-provided-secret-nsa-programs-for-hacking-scheme-accomplice.ashx>

Star, Y. D. T. D. (2018). Sehnaoui, accomplices indicted for hacking. The Daily Star. <http://www.dailystar.com.lb/News/Lebanon-News/2018/Oct-11/466010-sehnaoui-accomplices-indicted-for-hacking.ashx>

Brandom, R. (2018). Researchers have discovered a new kind of government spyware for hire. The Verge. <https://www.theverge.com/platform/amp/2018/1/18/16905464/spyware-lebanon-government-research-dark-caracal>

Paganini, P. (2018). Dark Caracal APT – Lebanese intelligence is spying on targets for years. Security Affairs. <https://securityaffairs.co/wordpress/67915/apt/dark-caracal-apt.html>

Arma. (2011, October 16). Trip report, Arab Bloggers Meeting, Oct 3-7. TorProject.org. <https://blog.torproject.org/blog/trip-report-arab-bloggers-meeting-oct-3-7>

Deepwebadmin. (2021). 11 Spine-Chilling and Nightmarish Deep Web Stories from Users. DeepWeb Sites 2021. <https://www.deepweb-sites.com/deep-web-stories/7/>

Schwindt, O. (n.d.). Epix's New Documentary Explores the Deep Web. TV Insider. <https://www.tvinsider.com/2884/epix-new-documentary-deep-web-ross-ulbricht/>

Greenberg, A. (2013). (n.d.). This machine kills secrets: how WikiLeaks, cypherpunks and hacktivists aim to free the world's information. Amazon. <https://www.amazon.com/This-Machine-Kills-Secrets-WikiLeakers/dp/0525953205>

Schwindt, O. (n.d.). Epix's New Documentary Explores the Deep Web. TV Insider. <https://www.tvinsider.com/2884/epix-new-documentary-deep-web-ross-ulbricht/>

Deep Web. (n.d.). Deep Web. Facebook. Retrieved May 13, 2021, from <https://www.facebook.com/deepwebmovie>

FreeRoss.org. (n.d.). Clemency for Ross Ulbricht, Serving Double Life for a Website. In Change.org. Retrieved May 30, 2021, from <https://www.change.org/p/president-of-the-united-states-clemency-for-ross-ulbricht-serving-double-life-for-a-website>

Suresh, Kalyani (2003). Theories of Communication. Professional Education, Testing and Certification Organization International. <http://www.peoi.org/Courses/Coursesen/mass/mass2.html>

Communication Theory. (n.d.). Authoritarian Theory. <https://www.communicationtheory.org/authoritarian-theory/>

Online Activity. (2020). CyberSouth: National Workshop on cybercrime procedural law in Lebanon. Council of Europe. <https://www.coe.int/en/web/cybercrime/-/cybersouth-national-workshop-on-cybercrime-procedural-law-in-lebanon>

Mahdi, H. (2019). Suzan is gone, but the bureau's violations persist. Beirut Today. <https://beirut-today.com/2019/04/04/cybercrime-bureau-violations/>

MODERN CYBERSECURITY: EDUCATIONAL AND TECHNICAL PERSPECTIVES. (2020). Beirut Arab University. <https://www.bau.edu.lb/International-Relations/MODERN-CYBERSECURITY?fbclid=IwAR1BS6ml3Y3PmKpjr7uAJzgK84aLB8n9gmfGGI36w11E8Xd-Qm-NHXX2eg8>

Kire. (2017). Tor usage worldwide: The Anonymous Internet. Digitale Gesellschaft. <https://www.digitale-gesellschaft.ch/2017/06/21/tor-usage-worldwide-the-anonymous-internet-new-infographic/>

Kemp, S. (2020). Digital 2020: Lebanon - DataReportal – Global Digital Insights. Data Reportal. <https://datareportal.com/reports/digital-2020-lebanon#:~:text=There%20were%205.35%20million%20internet,at%2078%25%20in%20January%202020>

Lebanon Population (n.d.). Worldometer. <https://www.worldometers.info/world-population/lebanon-population/#:~:text=Lebanon%202020%20population%20is%20estimated,of%20the%20total%20world%20population>

Barnard, A. (2013). Hezbollah's Role in Syria War Shakes the Lebanese. The New York Times. <https://www.nytimes.com/2013/05/21/world/middleeast/syria-developments.html>

DEBKAF. (2012). Iran's global cyber war-room is secretly hosted by Hizballah in Beirut. Wayback Machine. <https://web.archive.org/web/20121103181603/http://debka.com/article/22459/>

Blanford, N. (2008). Hezbollah phone network spat sparks Beirut street war. The Christian Science Monitor. <https://www.csmonitor.com/World/Middle-East/2008/0509/p05s01-wome.html>

OLJ. (2015). Affaire al-Jadeed : la directrice de l'association Arij invitée par la défense à témoigner. L'Orient-Le Jour. https://www.lorientlejour.com/article/924730/affaire-al-jadeed-la-directrice-de-lassociation-arj-invitee-par-la-defense-a-temoigner.html#_=_

About the investigation. (2018). International Consortium of Investigative Journalism. <https://www.icij.org/investigations/panama-papers/pages/panama-papers-about-the-investigation/>

"Giant leak of offshore financial records exposes global array of crime and corruption. (2016). OCCRP. <https://www.webcitation.org/6gVXG3LvI?url=https://www.occpr.org/en/panamapapers/overview/intro/>

Schmidt, M. S., & Myers, S. L. (2016). Panama Law Firm's Leaked Files Detail Offshore Accounts Tied to World Leaders. The New York Times. <https://www.nytimes.com/2016/04/04/us/politics/leaked-documents-offshore-accounts-putin.html>

"Помогут ли "Панамские документы" расставанию россиян с иллюзиями": СМИ обсуждают последствия "Офшоргейта" для РФ. (2016). NewsRU. <https://www.newsru.com/world/05apr2016/offshoregate.html>

"Вашего покорного слуги там нет": Путин прокомментировал "Панамские документы". (2016). NewsRU. <https://www.newsru.com/russia/07apr2016/putin.html>

O'Donovan, J., Wagner, H. F., & Zeume, S. (2019). Value of Offshore Secrets: Evidence from the Panama Papers. Oxford Academic. <https://academic.oup.com/rfs/article/32/11/4117/5315531>

Vaudano, M., & Michel, A. (2016). "Panama papers" : Panama, Vanuatu et Liban sont menacés de figurer sur la liste noire des paradis fiscaux. Le Monde. http://www.lemonde.fr/panama-papers/article/2016/04/16/panama-papers-panama-vanuatu-et-liban-sont-menaces-de-figurer-sur-la-liste-noire-des-paradis-fiscaux_4903528_4890278.html

Rabbah, M. (2020). من قتل جو بجاني؟. النهار العربي. <https://www.annaharar.com/arabic/makalat/opinions/24122020090419039>

(2019). BBC News launches 'dark web' Tor mirror. BBC. <https://www.bbc.com/news/technology-50150981>

Artificial Intelligence in Security and Defence. (2019). Lebanese Army. <https://www.lebarmy.gov.lb/sites/default/download/rssc2019/AISD2019-CFP-en.pdf>

Rabah, M. (2020). What photographer Joe Bejjani's death says about the dark days to come for Lebanon. Al Arabiya English. <https://english.alarabiya.net/views/news/middle-east/2020/12/23/What-photographer-Joe-Bejjani-s-death-says-about-the-dark-days-to-come-for-Lebanon>

BBC. (2021). Lokman Slim: Prominent Hezbollah critic shot dead in Lebanon. BBC. <https://www.bbc.com/news/world-middle-east-55933222>

Bunkley, N. (2008). Joseph Juran, 103, Pioneer in Quality Control, Dies. The New York Times. <https://www.nytimes.com/2008/03/03/business/03juran.html>

BBC. (2019). BBC News launches 'dark web' Tor mirror. BBC. <https://www.bbc.com/news/technology-50150981>

BBC. (2019). BBC News launches 'dark web' Tor mirror. BBC. <https://www.bbc.com/news/technology-50150981>

Lexico Dictionaries. (n.d.). Activist. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/activist>

Lexico Dictionaries. (n.d.). Anarchist. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/anarchist>

Lexico Dictionaries. (n.d.). Anarchy. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/anarchy>

Techopedia. (2011). Anonymizer. In Techopedia.com. Retrieved May 13, 2021, from <https://www.techopedia.com/definition/23133/anonymizer>

Cambridge Dictionary. (n.d.). Aphorism. In Cambridge.org dictionary. Retrieved May 13, 2021, from <https://dictionary.cambridge.org/dictionary/english/aphorism>

Oxford Learner's Dictionary. (n.d.). Appalling. In OxfordLearnersDictionaries.com dictionary. Retrieved May 13, 2021, from <https://www.oxfordlearnersdictionaries.com/definition/english/appalling>

Lexico Dictionaries. (n.d.). Authoritarianism. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/authoritarianism>

Posey, B. (2021). (n.d.). Backdoor. In TechTarget.com. Retrieved May 13, 2021, from <https://searchsecurity.techtarget.com/definition/back-door>

Merriam-Webster. (n.d.). Beacon. In Merriam-Webster.com dictionary. Retrieved May 13, 2021, from <https://www.merriam-webster.com/dictionary/beacon>

Lexico Dictionaries. (n.d.). Bitcoin. In Lexico.com dictionary. Retrieved May 13, 2021, from <https://www.lexico.com/definition/bitcoin>

Lexico Dictionaries. (n.d.). Blockchain. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/blockchain>

Lexico Dictionaries. (n.d.). Blog. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/blog>

Lexico Dictionaries. (n.d.). Web browser. In Lexico.com dictionary. Retrieved May 13, 2021, from https://www.lexico.com/definition/web_browser

Merriam-Webster. (n.d.). Blue Screen Of Death. In Merriam-Webster.com dictionary. Retrieved May 13, 2021, from <https://www.merriam-webster.com/dictionary/blue%20screen%20of%20death>

Lexico Dictionaries. (n.d.). Bureaucracy. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/bureaucracy>

Lexico Dictionaries. (n.d.). Censorship. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/censorship>

Lexico Dictionaries. (n.d.). Chatbot. In Lexico.com dictionary. Retrieved May 13, 2021, from <https://www.lexico.com/definition/chatbot>

Merriam-Webster. (n.d.). Chat Room. In Merriam-Webster.com dictionary. Retrieved May 13, 2021, from <https://www.merriam-webster.com/dictionary/chat%20room>

Encyclopedia.com. (2021). Classified information. In Encyclopedia.com. Retrieved May 13, 2021, from <https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/classified-information>

Urban Dictionary. (n.d.). Clearnet. In OxfordDictionaries.com dictionary. Retrieved May 13, 2021, from <https://www.urbandictionary.com/define.php?term=clearnet>

Lexico Dictionaries. (n.d.). Cloud computing. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/cloud%20computing>

Frankenfield, J. (2020). Cloud security. In Investopedia.com dictionary. Retrieved May 13, 2021, from <https://www.investopedia.com/terms/c/cloud-security.asp>

Encyclopædia Britannica, inc. (n.d.). Computer network. In Britannica.com dictionary. Retrieved May 13, 2021, from <https://www.britannica.com/technology/computer-network>

Lexico Dictionaries. (n.d.). Constitution. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/constitution>

Legal Information Institute. (n.d.). Contempt of Court. In Law.Cornell.edu. Retrieved May 13, 2021, from https://www.law.cornell.edu/wex/contempt_of_court

Urban Dictionary. (n.d.). Creepypasta. In UrbanDictionary.com dictionary. Retrieved May 13, 2021, from <https://www.urbandictionary.com/define.php?term=Creepypasta>

Lexico Dictionaries. (n.d.). Cryptanalysis. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/cryptanalysis>

Lexico Dictionaries. (n.d.). Cryptocurrency. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/cryptocurrency>

Lexico Dictionaries. (n.d.). Cyber. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/cyber>

Lexico Dictionaries. (n.d.). Cybercrime. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/cybercrime>

VMware Carbon Black. (n.d.). Cyber Espionage. In CarbonBlack.com. Retrieved May 13, 2021, from <https://www.carbonblack.com/resources/definitions/what-is-cyber-espionage/>

Techopedia. (2012). Cyberlaw. In Techopedia.com. Retrieved May 13, 2021, from <https://www.techopedia.com/definition/25600/cyberlaw>

Cisco. (2020). Cybersecurity. In Cisco.com. Retrieved May 13, 2021, from <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>

Lexico Dictionaries. (n.d.). Cyberspace. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/cyberspace>

Lexico Dictionaries. (n.d.). Cybercriminal. In Lexico.com dictionary. Retrieved May 13, 2021, from <https://www.lexico.com/definition/cybercriminal>

Lexico Dictionaries. (n.d.). Cyberwarfare. In Lexico.com dictionary. Retrieved May 30, 2021, from <https://www.lexico.com/definition/cyberwarfare>

Lexico Dictionaries. (n.d.). Cypherpunk. In Lexico.com dictionary. Retrieved May 13, 2021, from <https://www.lexico.com/definition/cypherpunk>

Contributor, T. T. (2005). Daisy chain. In WhatIs.TechTarget.com. Retrieved May 13, 2021, from <https://searchnetworking.techtarget.com/definition/daisy-chain>

Twin, A. (2021). Data Mining. In Investopedia.com. Retrieved May 13, 2021, from <https://www.investopedia.com/terms/d/datamining.asp>

Lexico Dictionaries. (n.d.). Dark web. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/Dark%20Web>

Lexico Dictionaries. (n.d.). Darknet. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/darknet>

Frankenfield, J. (2020). Deep Web. In Investopedia.com. Retrieved May 13, 2021, from <https://www.investopedia.com/terms/d/deep-web.asp>

Lexico Dictionaries. (n.d.). Defamation. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/defamation>

HarperCollins Publishers Ltd. (n.d.). Defendant. In CollinsDictionary.com. Retrieved May 13, 2021, from <https://www.collinsdictionary.com/dictionary/english/defendant>

Palo Alto Networks. (n.d.). Denial of service attack. In PaloAltoNetworks.com. Retrieved May 13, 2021, from <https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos>

Kagan, J. (2021). Digital wallet. In Investopedia.com. Retrieved May 13, 2021, from <https://www.investopedia.com/terms/d/digital-wallet.asp>

Cambridge Dictionary. (n.d.). Dissident. In Dictionary.Cambridge.com. Retrieved May 13, 2021, from <https://dictionary.cambridge.org/dictionary/english/dissident>

Lexico Dictionaries. (n.d.). Drone. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/drone>

Lexico Dictionaries. (n.d.). Eagle scout. In Lexico.com dictionary. Retrieved May 30, 2021, from https://www.lexico.com/definition/eagle_scout

Merriam-Webster. (n.d.). Eavesdrop. In Merriam-Webster.com dictionary. Retrieved May 13, 2021, from <https://www.merriam-webster.com/dictionary/eavesdrop>

Lexico Dictionaries. (n.d.). Echelon. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/echelon>

Lexico Dictionaries. (n.d.). Edict. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/edict>

NCSC. (n.d.). Penetration testing. In NCSC.gov.uk. Retrieved May 13, 2021, from <https://www.ncsc.gov.uk/guidance/penetration-testing>

Lexico Dictionaries. (n.d.). Encryption. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/encryption>

Dictionary.com. (n.d.). Epiphany. In Dictionary.com dictionary. Retrieved May 13, 2021, from <https://www.dictionary.com/browse/epiphany>

Lexico Dictionaries. (n.d.). Espionage. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/espionage>

Greycampus. (n.d.). Ethical Hacking. In GreyCampus.com. Retrieved May 13, 2021, from <https://www.greycampus.com/opencampus/ethical-hacking/what-is-ethical-hacking>

Legal Information Institute. (n.d.). Exculpatory Evidence. In Law.Cornell.edu. Retrieved May 13, 2021, from https://www.law.cornell.edu/wex/exculpatory_evidence

Cambridge Dictionary. (n.d.). Felony. In Dictionary.Cambridge.org. Retrieved May 13, 2021, from <https://dictionary.cambridge.org/dictionary/english/felony>

Keysight Technologies. (n.d.). Traffic filtering. In Blogs.Keysight.com. Retrieved May 13, 2021, from https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2020/04/30/traffic_filtering-ILFq.html

Cisco. (2021). Firewall. In Cisco.com. Retrieved May 13, 2021, from <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>

Cambridge Dictionary. (n.d.). Flounder. In Dictionary.Cambridge.com. Retrieved May 13, 2021, from <https://dictionary.cambridge.org/dictionary/english/flounder>

Lexico Dictionaries. (n.d.). Forum. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/forum>

Lexico Dictionaries. (n.d.). The fourth estate. In Lexico.com dictionary. Retrieved May 13, 2021, from https://www.lexico.com/definition/the_fourth_estate

Lexico Dictionaries. (n.d.). Glocal. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/glocal>

Lexico Dictionaries. (n.d.). Hacking. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/hacking>

Lexico Dictionaries. (n.d.). Hacktivist. In Lexico.com dictionary. Retrieved May 13, 2021, from <https://www.lexico.com/definition/hacktivist>

Cambridge Dictionary. Hitherto. In Dictionary.Cambridge.com. Retrieved May 13, 2021, from <https://dictionary.cambridge.org/dictionary/english/hitherto>

Lexico Dictionaries. (n.d.). Iconoclast. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/iconoclast>

HarperCollins Publishers Ltd. (n.d.). In flagrante delicto. In CollinsDictionary.com. Retrieved May 13, 2021, from <https://www.collinsdictionary.com/dictionary/english/in-flagrante-delicto>

Sam Marsden. (2021). Search engine indexing. In DeepCrawl.com. Retrieved May 13, 2021, from <https://www.deepcrawl.com/knowledge/technical-seo-library/search-engine-indexing/>

Lexico Dictionaries. (n.d.). Indict. In Lexico.com dictionary. Retrieved May 13, 2021, from <https://www.lexico.com/definition/indict>

Lexico Dictionaries. (n.d.). Infiltrate. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/infiltrate>

Lexico Dictionaries. (n.d.). Informatics. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/informatics>

Legal Information Institute. (n.d.). Intellectual property. In Law.Cornell.edu. Retrieved May 13, 2021, from https://www.law.cornell.edu/wex/intellectual_property

PCMag. (n.d.). Internet domain name. In PCMag.com. Retrieved May 13, 2021, from <https://www.pcmag.com/encyclopedia/term/internet-domain-name>

Internet Governance Project. (2018). Internet governance. In InternetGovernance.org. Retrieved May 13, 2021, from <https://www.internetgovernance.org/what-is-internet-governance/>

Burgess, M. (n.d.). Internet of things. In Wired.co.uk. Retrieved May 13, 2021, from <https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot>

Encyclopædia Britannica, inc. (n.d.). Internet service provider. In Britannica. Retrieved May 13, 2021, from <https://www.britannica.com/technology/Internet-service-provider>

UNESCO. (2018). Investigative journalism. In UNESCO.org. Retrieved May 13, 2021, from <https://en.unesco.org/investigative-journalism>

Lexico Dictionaries. (n.d.). IP address. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/IP%20address>

Dictionary. (n.d.). Jurisprudence. In Dictionary.com. Retrieved May 13, 2021, from <https://www.dictionary.com/browse/jurisprudence>

Merriam-Webster. (n.d.). Kingpin. In Merriam-Webster.com dictionary. Retrieved May 13, 2021, from <https://www.merriam-webster.com/dictionary/kingpin>

Salami E. (2017). Legal Informatics. In SSRN.com. Retrieved May 13, 2021, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2966201

Lexico Dictionaries. (n.d.). Legislate. In Lexico.com dictionary. Retrieved May 13, 2021, from <https://www.lexico.com/definition/legislate>

Encyclopædia Britannica, inc. (n.d.). Libertarianism. In Britannica.com. Retrieved May 13, 2021, from <https://www.britannica.com/topic/libertarianism-politics>

Lexico Dictionaries. (n.d.). Mandate. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/mandate>

Lexico Dictionaries. (n.d.). Marketplace. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/marketplace>

Encyclopædia Britannica, inc. (n.d.). Mental hygiene. In Britannica.com. Retrieved May 13, 2021, from <https://www.britannica.com/science/mental-hygiene>

International Commission of Jurists. (2018). Military court of cassation. In ICJ.org. Retrieved May 13, 2021, from <https://www.icj.org/wp-content/uploads/2018/05/Lebanon-Memoire-army-courts-Advocacy-Analysis-Brief-2018-ENG.pdf>

Techopedia. (2011). Mobile network operator. In Techopedia.com. Retrieved May 13, 2021, from <https://www.techopedia.com/definition/27804/mobile-network-operator-mno>

Lexico Dictionaries. (n.d.). Narcotic. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/narcotic>

Legal Information Institute. (n.d.). Obstruction of justice. In Law.Cornell.edu. Retrieved May 13, 2021, from https://www.law.cornell.edu/wex/obstruction_of_justice

PCMag. (n.d.). Onion domain. In PCMag.com. Retrieved May 13, 2021, from <https://www.pcmag.com/encyclopedia/term/onion-domain>

Merriam-Webster. (n.d.). Outdoorsman. In Merriam-Webster.com dictionary. Retrieved May 13, 2021, from <https://www.merriam-webster.com/dictionary/outdoorsman>

Geere, D. (2021). Packet inspection. In Wired.co.uk. Retrieved May 13, 2021, from <https://www.wired.co.uk/article/how-deep-packet-inspection-works>

Fruhlinger, J. (2020). Phishing. In CSO Online.com. Retrieved May 13, 2021, from <https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html>

Lexico Dictionaries. (n.d.). Piracy. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/piracy>

Torre, L. F. de la. (2020). Privacy by design. In Medium.com. Retrieved May 13, 2021, from <https://medium.com/golden-data/what-is-privacy-by-design-pbd-9a3e4d96536a>

Lexico Dictionaries. (n.d.). Prosecute. In Lexico.com dictionary. Retrieved May 13, 2021, from <https://www.lexico.com/definition/prosecute>

Merriam-Webster. (n.d.). Prosecuting Attorney. In Merriam-Webster.com dictionary. Retrieved May 13, 2021, from <https://www.merriam-webster.com/dictionary/prosecuting%20attorney>

Lexico Dictionaries. (n.d.). Ransom. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/ransom>

Legal Dictionary. (n.d.). Repudiation. In Dictionary.Law.com. Retrieved May 13, 2021, from <https://dictionary.law.com/Default.aspx?selected=1804#:~:text=repudiation,to%20perform%20a%20contract%20obligation>

Tech Terms Dictionary. (n.d.). Script. In TechTerms.com dictionary. Retrieved May 13, 2021, from <https://techterms.com/definition/script>

Lexico Dictionaries. (n.d.). Search engine. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/search%20engine>

Lexico Dictionaries. (n.d.). Serial number. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/serial%20number>

Merriam-Webster. (n.d.). Sleeper Cell. In Merriam-Webster.com dictionary. Retrieved May 13, 2021, from <https://www.merriam-webster.com/dictionary/sleeper%20cell>

OmniSecu. (n.d.). Sniffer attack. In OmniSecu.com. Retrieved May 13, 2021, from <http://www.omnisecu.com/security/sniffer-attack.php>

Lexico Dictionaries. (n.d.). Spyware. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/spyware>

PCMag. (n.d.). Surface web. In PCMag.com. Retrieved May 13, 2021, from <https://www.pcmag.com/encyclopedia/term/surface-web>

Lexico Dictionaries. (n.d.). Takfiri. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/Takfiri>

Kagan, J. (2021). Tax haven. In Investopedia.com. Retrieved May 13, 2021, from <https://www.investopedia.com/terms/t/taxhaven.asp>

Lexico Dictionaries. (n.d.). Testify. In Lexico.com dictionary. Retrieved May 13, 2021, from <https://www.lexico.com/definition/testify>

Frankenfield, J. (2020). Tor. In Investopedia.com. Retrieved May 13, 2021, from <https://www.investopedia.com/terms/t/tor.asp>

Techopedia. (2016). Network traffic analysis. In Techopedia.com. Retrieved May 13, 2021, from <https://www.techopedia.com/definition/29976/network-traffic-analysis>

Froehlich, A. (2020). (n.d.). Traffic Shaping. In TechTarget.com. Retrieved May 13, 2021, from <https://searchnetworking.techtarget.com/definition/traffic-shaping>

Oxford Advanced Learner's Dictionary. (n.d.). Travesty. In OxfordLearnersDictionaries.com. Retrieved May 13, 2021, from <https://www.oxfordlearnersdictionaries.com/definition/english/travesty>

Lexico Dictionaries. (n.d.). Uncanny. In Lexico.com dictionary. Retrieved May 13, 2021, from <https://www.lexico.com/definition/uncanny>

Lexico Dictionaries. (n.d.). UAV. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/UAV>

Techopedia. (2021). Uniform Resource Locator. In Techopedia.com. Retrieved May 13, 2021, from <https://www.techopedia.com/definition/1352/uniform-resource-locator-url>

Lexico Dictionaries. (n.d.). User interface. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/user%20interface>

Lexico Dictionaries. (n.d.). Vet. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/vet>

VMware. (n.d.). Virtual Machine. In VMware.com. Retrieved May 13, 2021, from https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc_50%2FGUID-CEFF6D89-8C19-4143-8C26-4B6D6734D2CB.html

Cisco. (2020). VPN. In Cisco.com. Retrieved May 13, 2021, from <https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html>

Lexico Dictionaries. (n.d.). Warrant. In Lexico.com dictionary. Retrieved May 29, 2021, from <https://www.lexico.com/definition/warrant>

Tech Terms Dictionary. (n.d.). Web browser. In TechTerms.com dictionary. Retrieved May 13, 2021, from https://techterms.com/definition/web_browser

IGI Global. (n.d.). Web interface. In IGI-Global.com. Retrieved May 13, 2021, from <https://www.igi-global.com/dictionary/web-interface/37135>

Merriam-Webster. (n.d.). Whistleblower. In Merriam-Webster.com dictionary. Retrieved May 13, 2021, from <https://www.merriam-webster.com/dictionary/whistleblower>

Lexico Dictionaries. (n.d.). White hat. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/white%20hat>

Lexico Dictionaries. (n.d.). Wiki. In Lexico.com dictionary. Retrieved May 13, 2021, from <http://english.oxforddictionaries.com/wiki>

Appendix A

Horror story: Who is Janice?

The job offer: when Mark Spielman knew that the local police was looking to hire a person who had in-depth knowledge of the internet, he grabbed the opportunity.

An uncanny* discovery: “Like any other day, he was looking at some CP (child pornography) sites and found disturbing to take a look at these often. Found a website with a URL* called “Sweet15.com”. One of the biggest CP sites he has never seen and started digging into the website content. He browsed on a random page and clicked on the image link called “Cathy.jpg”. “It was a picture of a young girl with long hair and pale skin, about 15 or 16, standing in a dimly lit room with a smile on her face. Not a full, toothy smile, but just a slight grin.” But after seeing the name of the image it was not “cathy.jpg” but it was “janice.jpg”. Now decided to click on “Susan.jpg” but ended in the same image even after clicking 15 to 20 files. Even a video “PennyPrecious.wav” ended in the same place. With help of his office colleagues, he researched it but all ended in the same place. Left the office after frustration and found something was missing and he did not really thoroughly check it.

Following the clues, and soon after he reached home started working on it and found on the very last page of the picture file logs was a lone picture file called “TrueJanice.jpg”. He clicked on it then the computer crashed and shut down with the BSOD* [blue screen of death]. Later he turned it on after quite a time trying and found that all his programs were deleted and found 1000’s of image files copied with the most shocking thing is that the desktop image was “Janice.jpg”. In mixed feelings of fear and uncontrollable interest he started clicking on one image at a time. He says “It was Janice.jpg,

the black-and-white photo. Something about Janice's facial expression was different, though." The first images were exactly the same but after some clicks, it had morphed into the frowning one that was on the desktop. Few rapid clicks revealed that she starts to confront into a scream.

The following came to his shock when several 100 clicks the screen turned black and suddenly saw a bundle on the bed with a blanket on the top and he explained "The scene was in a dark room with a few candles burning to light it up. I noticed in horror that there were red splotches on the wall behind the bed, which was what I knew had to be blood." Few more pictures clicked a man walked into the frame with surgical instruments and cut open the girl's stomach and started ripping out her guts, piece by piece and it was so bloody and vivid. Now he was on the 995 of 1000 pictures and started moving slowly from one pic to the next pic. In 998, I saw a grainy photo of a young girl staring at me. Her eyes were blank, expressionless. I couldn't see much, so I went on to picture 999. I could then see what the picture was. I was face-to-face with Janice. She was covered in blood and I knew she was dead already. The last photo had a black background with a large question mark in the center and below with a simple question "Who is Janice?".

Afterwards, the official statement given by the police department was: "Officers found this document on Detective Mark Spielman's hard drive. We found this document stored on his computer along with what appears to be a note. All that the note said was "WHO IS JANICE?!" After going over the files on his computer, we found several documents pertaining as to who Janice may have been". "From what we can gather, she had been kidnapped from her family around 20 years ago. She was never found. Her parents vanished shortly after the kidnapping. Upon further investigation, officers found computer

code embedded in her picture”. “From what we could gather, it was a scrambled bit of code that, when deciphered, linked to a video file. However, upon viewing the file, the investigating officers deleted it and refused to divulge what they had seen. Mark Spielman was never found. The case has since been discontinued.”

Appendix B

Deep Web (2015 documentary) (<http://www.deepwebthemovie.com/>)

A True Story

On January 13th, 2015, a criminal trial began for the accused leader of the Silk Road, which popped up on the dark web in 2011 as a black market for just about any illegal good or service one could think up: Ross Ulbricht, a 30-year-old entrepreneur who was arrested while logged-in to Silk Road as an administrator, admitted to being the creator of Silk Road, and was convicted in February on various counts of drug trafficking and money laundering. However, the trial of Ross Ulbricht raised more questions than it answered, with the case setting a precedent for the warrantless* search of Americans' digital property, which is an illegal act that has allegedly been committed by law enforcement to catch Ulbricht “in flagrante delicto”.

But earlier in life, Ross William Ulbricht could not be more different than those allegations: growing up in Texas, USA in a middle-class family, he was an avid outdoorsman*, an Eagle Scout* like his father, who displayed an early attitude for math, and who earned a full scholarship to the University of Texas, studying physics. He graduated in 2006, and then won another full scholarship in Pennsylvania State University in materials science and engineering: it was at Pennsylvania State University that Ross began a deep interest in libertarianism*, and after completing his masters in 2009, he told his mother that he no longer had an interest in pursuing a career in science, and instead wanted to become an entrepreneur: he opened his own used book company, donating a portion of the proceeds to a youth program and to a prison literacy project. But the business floundered*, and Ross had to shut it down, and if a post on his LinkedIn page was of any indication, he

experienced a kind of epiphany* on his next way forward: “I love learning and using theoretical constructs to better understand the world around me. Naturally therefore, I studied physics in college and worked as a research scientist for five years. My goal during this period of my life was simply to expand the frontier of human knowledge. Now, my goals have shifted. I want to use economic theory as a means to abolish the use of coercion and aggression amongst mankind. The most widespread and systemic use of force is amongst institutions and governments, so this is my current point of effort. The best way to change a government is to change the minds of the governed, however. To that end, I am creating an economic simulation to give people a first-hand experience of what it would be like to live in a world without the systemic use of force”.

An interview with Ross’s parents – Kirk and Lyn – brings surprising claims to the table: "We've had regular meetings with Josh (Joshua Dratel, the attorney of Ross Ulbricht), we know that his witnesses were blocked from testifying*. We were in the courtroom, and we saw the travesty*, the appalling* obstruction of justice that happened. There was 5000 pages of government evidence to do with one witness alone, none of that was allowed, 5000 pages and it was dumped on the defense ten days before trial. Another 2500 pages for other witnesses was dumped on the defense a week before trial, and it was full of exculpatory evidence* favorable to Ross and that was not permitted to be used. All this great, huge field of evidence that came out in the 3500 materials a week before trial, that would help prove Ross's innocence, was excluded from being brought out in the courtroom. It would have been a whole different case. This was the trial that didn't happen because there was only the prosecution's narrative that we heard."

Moving on to Andy Greenberg, a senior writer at Wired magazine, he got the chance to run an e-mail based interview with Ross before the latter got caught, during which time Greenberg was approaching the administrator (or one of the multiple administrators who consecutively ran Silk Road), therefore the identity of Ulbricht was still unknown: when Greenberg was later asked if the US government hacked the foreign servers of the Silk Road in order to catch Ross, he replies with the following: “We didn't get that far, we didn't get to even have that kind of public hearing where the FBI has to say how they did it and then we get to decide whether that was legal or illegal. It's maybe the most frustrating thing about this case from a legal point of view that, American law enforcement hacked a foreign server, I believe, and they didn't have a warrant, and they completely got away with it, nobody even gets to ask a question about it. Ross Ulbricht is a fascinating character, he invented this brilliant thing (Silk Road), he had principles, he wasn't just a cybercriminal*, he wasn't just a drug lord or a kingpin* as he's described in the charges, and he was also an idealistic guy, and I'm gonna be conflicted about both the kind of virtue of the Silk Road and of Ross Ulbricht as a person I think for the rest of my life, I'm not gonna be able to come to a conclusion about this”.

Even a Baltimore Police major talked about how Silk Road helped reduce drug-related violence, claiming that it protected clients from the risk of meeting directly with drug dealers, and it also increased the accountability of e-sellers through marketplace reviews.

End of a story / beginning of a journey: whatever the ultimate outcome, it was clear that the fall of the Silk Road was not the end of a chapter but the beginning, and the movement to create tools and services for online privacy is stronger than ever; the documentary ends with the caption “Criminal charges were brought against two senior FBI agents on the

Baltimore Silk Road Task Force on March 25, 2015. Among other things, they were accused of stealing over a million dollars' worth of bitcoins from Silk Road and transferring them to private accounts. By order of the government for Ulbricht's defense, this investigation was not allowed during the hearing. On May 29, 2015, Ross Ulbricht was sentenced to life imprisonment without parole". It is worth noting that the documentary aired on May 31, 2015, just two days after the sentencing. After the above caption, a flashback to before Ross got arrested, he was asked in an interview about his plans 20 years from that date, and he replies "I wanna have a substantial positive impact on the future of humanity" and he continues to say that with the current rate of technological advancement, he thinks that it is a possibility that he is going to live forever "in some form", which clearly shows his unrelenting attitude.

The Production Team

Alex Winter (writer, director, producer): when asked if he got to speak to Ross at all, since the latter only appears in the movie through secondary footage, Alex Winter replies: "I wasn't allowed any access at all. It was somewhat to do with the prison system and the severity of the charges that he was not going to be filmed by anybody. And also, I gotta be totally honest with you, it wasn't something I was pushing for. I didn't want to become biased. I have compassion for the family, and I think that shows. And I do have compassion for anybody who's caught in the middle of something this complex."

Andy Greenberg (consulting producer): he appears in the movie which includes select source material from "This Machine Kills Secrets", a 2012 book by Greenberg about "how wikileaks, cypherpunks*, and hacktivists* aim to free the world's information". Speaking of WikiLeaks, the movie also features old footage of the struggle that Julian Assange faced

against political oppression, perhaps unsurprisingly considering his work being at the intersection of the dark web with freedom of speech. Andy Greenberg is also a senior writer for Wired and a former staff writer for Forbes: his Forbes story on WikiLeaks and the future of information leaks in late 2010 was the first magazine cover story to feature Julian Assange. In 2013, he became the only journalist to interview the secretive administrator of the Silk Road black market known as the Dread Pirate Roberts (who was later proven by law enforcement to be none other than Ross Ulbricht). And his Forbes cover story later that year on data mining firm Palantir was selected as a Gerald Loeb Award finalist for best magazine feature.

Keanu Reeves (narrator): according to director Alex Winter, “Keanu had been sort of a consulting producer all along, he’d been present during the process, so it was a fairly easy ask [to have him as narrator].”

Impact: media outlets that mentioned the movie: HuffPostLive, MSNBC, The Huffington Post, The Daily Dot, Wired, Laughing Squid, Vocativ, Mashable, TheVerge, DeadLine.com, Bloomberg Television, Yahoo!, CNN International, Nerdist, USAToday.com, CNET, IndieWire, Business Insider, FilmSchoolRejects, The Kernel, Empire, Motherboard, Twitch...

Objectivity statement: the producers’ bias shows on their Facebook page through a post that is dated February 25, 2020, five years after the release of the movie and the sentencing of Ulbricht: “A reminder that Ross Ulbricht is serving a double life sentence for his part in the Silk Road. It's an egregious sentence, whatever you think of the charges, it sets a terrible precedent in cyber and drug war cases.” This post also links to a Change.org petition entitled “Clemency for Ross Ulbricht, Serving Double Life for a Website”, and

which was started by FreeRoss.org, an organization in which the Ulbricht family is actively involved.

After the creation and destruction of Silk Road 1.0, Silk Road 2.0 quickly emerged afterward and was also taken down by the feds, but Silk Road 3.0 lives on, proving how unregulatable the dark web truly is. The documentary even quotes a police statement, that the dark web cannot be stopped, and thus will continue to proliferate, ceaselessly, until it revolutionizes the world...

The hero-criminal / evil-prosecutor dilemma: this media production blurs the line for anyone trying to reach a satisfying conclusion as to whom is the real protagonist and who is the antagonist, in a mind-bending plot.

Ross Ulbricht	Law enforcement
Running an illegal marketplace Caught while in the act of operating Silk Road Smart guy with bright ambitions Protecting drug consumers from meeting with the sellers, thus reducing street violence Serving a double life sentence	Making sure that the law is abided Selectively excluding evidence from trials Corrupt policemen stealing from Silk Road Protecting society from trading illegal goods, regardless of the medium (offline/online) Ruling their country unquestionably

Putting the Silk Road story in context, and if the trials of Ross Ulbricht were indeed unfair, in America where cybercrime laws are present, little remains left to the imagination as to how fair a similar trial would take place in Lebanon, where no such laws exist and where decades of corruption corroded its judicial system, along with all of its public institutions. Drawing the analogy between this story which happened in the USA, with the case of Ziad Itani in Lebanon, the witnesses of Ross Ulbricht were not allowed to testify in court, just like the fact that Itani was never asked by the “military court of cassation” to testify as a witness in the Hajj Hobeich case.