

# Coronavirus Conspiracies and Dis/Misinformation on the Dark Web

Written by Lev Topor and Pnina Shuker

This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

## Coronavirus Conspiracies and Dis/Misinformation on the Dark Web

<https://www.e-ir.info/2020/10/09/coronavirus-conspiracies-and-dis-misinformation-on-the-dark-web/>

LEV TOPOR AND PNINA SHUKER, OCT 9 2020

In this article we examine the spread of dis/misinformation on the dark web, mainly on The Onion Router (TOR) platform, in the context of direct and proxy spread (in-direct) of information. We also suggest that the dark web can be used by global powers to intensify the disinformation campaign waged on conventional media and on social media. As the true origin of dark web information is extremely difficult to identify, we suggest that some of this information was promoted by global powers and some by extremists and propagandists. Interestingly, in the case of the pandemic, these two forces (States and propagandists) complement each other and cause social chaos, this deepens the authority crisis and makes internet users and their social circuits more prone to believing conspiracies. Moreover, this unreliable spread of information can make the virus even more lethal as those who consume and believe disinformation and conspiracy are more likely to disobey quarantine, restrictions and other medical and public health regulations. This fact makes the dark side of our internet even more dangerous.

The regular internet is now an integral part of our lives for about three consecutive decades, it has shifted traditional practices and created new trends on all aspects of life, including globalization, citizenship, socialization, economy and much more. It had even become a new battleground for international actors. The internet, in essence, helped people and domains worldwide to connect in 'reality' and in cyberspace. However, we now face a difficult situation as the COVID-19 (Coronavirus) crisis had shifted some trends backwards – people are now segregated and restricted, yet people are also drowning in an influx of information, about which they cannot discuss or act on traditional social (physical) terms. That is, internet users are facing a difficult problem of signaling out truth, facts, from fiction or conspiracy. Since people worldwide have no real interactions with others, and with [the] authorities, they are now positioned in a vacuum, which is causing a very significant authority crisis to emerge, especially in the West.

### Methodology

In order to examine the topic effectively, considering technological constraints affiliated with dark web data gathering, a qualitative study of ethnographic nature was chosen. The methodology was also endorsed by the cyber and intelligence company OTB Intelligence Ltd which one of the authors is affiliated with. A set of preliminary interviews with cyber and intelligence consultants was made, afterwards, the most popular dark web sites, blogs, forums and boards were identified (only on TOR). Further, a keyword list was built for use. The list was also verified in Google Trends. The information was also compared to search trends found on SimilarWeb and the initiative between Google, Schema and AXIOS as well as comparisons for Facebook trends.

The websites on the dark web are mentioned in the article and the initial keywords used for this research are: COVID-19, Coronavirus, Virus, Plague, Pandemic, Epidemic, Spread, Biological Weapon, Respiratory, Trade War, Conspiracy, Plot, Lockdown, Outbreak, Social Distance, Fomite, Quarantine, Isolation, Infection, N95. The search was also made in Russian with the words: Коронавирус, Пандемия, мор, Грипп, Карантин, Конспирация. A limited search was also made for Chinese words: 冠状病毒, 疫情, 阴谋. Other variations were used in English as well, for instance, change of signs, letters, and so on.

Some important findings are documented with screen shots for further proof and use. Dark web data collection is

# Coronavirus Conspiracies and Dis/Misinformation on the Dark Web

Written by Lev Topor and Pnina Shuker

problematic since websites, IPs, DNSs, ports and codes frequently change. Additionally, even though the largest search and gathering was done in English due to restrictions of time and resources, most of the dark web users communicate in English and it can be assumed that the dis/misinformation is aimed mainly at the West (English speaking countries and users). Thus, we can assume that even with unlimited resources most of the information is presented in English in any case though further inquiry into the matter would give more detailed insights.

## Perception of Information and How Global Powers Use It

[Unreliable] Information on the internet is dangerous not just because it spreads quickly and widely. It is also dangerous because users, people, are more likely to believe a story which they heard from an actual in-person conversation. In fact, a certain story might be perceived by an internet user as a lie if it was read online, however, it might be perceived by that same user as something truthful if it was argued by an actual person or even an authority figure. The internet has not made people more prone to conspiracies. That is, unless the conspiracy was argued by a third-party proxy – a party which is perceived as trustworthy in reality. Thus, as we further articulate, the danger with dark web information is not its direct spread but its proxy, or in-direct, spread.

The spread by proxy is an even greater problem regarding the dark web – an overlay network, a web which requires a certain software and connection configurations. Information on the dark web is perceived by many internet users to be authentic, truer than information on traditional platforms like official press releases by governments or reputable printed media – these are sometimes perceived to be driven by state interests that do not always align with the interests of citizens. With the outbreak of the COVID-19 pandemic the perception and use of information on the dark web is even more intriguing since information operations in the cyber domain became more prominent between global adversaries which create entire ecosystems to facilitate their campaigns.

Moreover, with the proliferation of the pandemic, related conspiracy theories have emerged, pushing international actors that do not want to waste a good crisis, into exploiting the pandemic for their own strategic international and even domestic goals. In the international arena, actor A defames actor B with mis/disinformation to weaken him, which, subsequently, makes actor A more powerful. In the domestic arena, rulers and politicians alike blame outside threats for their own mismanagement. Thus, various global forces are also taking advantage of privacy and anonymity of the dark web.

The coronavirus pandemic did not initiate tensions between global powers, which battle over the global premier for years. Mainly, it has further inflamed US-China tensions, with both sides blaming the other for the spread of the virus. Beijing has denied that the virus originated in China and blamed the US for the spread of the virus. China's Foreign Ministry spokesperson, Zhao Lijian, said that the US is attempting to defame the Chinese government, shift responsibility and find a scapegoat. In turn, the US administration begun referring to coronavirus as the 'Chinese virus'.

Following US rhetoric, restrictions on Chinese diplomats, and the ongoing trade war and negotiations between the two, Beijing launched an active public relations campaign to say that the virus did not originate in China. Chinese diplomats worldwide are being instructed to assign the virus as something else, such as an 'Italian Virus' or 'Iranian Virus'. Zhao Lijian even claimed the virus may have originated in the US and have been brought to China by the US military.

The US responded to the Chinese information campaign in order to block Chinese accusations. The US campaign to counter China's one included mostly blaming and criticizing China for its delayed and non-transparent response against the Coronavirus. A bipartisan resolution has been introduced in the US, condemning the Chinese government over its handling of the outbreak, painting a stark picture of lies and mismanagement which contributed to the pandemic.

Russia also joined the spread of fake news and dis/misinformation, further expanding its ongoing state-sponsored disinformation campaigns. Russia has deployed fake news to sow panic in West, as part of a broader strategic campaign to weaken its adversaries.

# Coronavirus Conspiracies and Dis/Misinformation on the Dark Web

Written by Lev Topor and Pnina Shuker

Iran, a Chinese and Russian ally, has also made political and strategic use of the coronavirus. The Iranian regime has spread the conspiracy theory that the US, Israel and even the Jews are behind the virus. The Iranian Revolutionary Guards Corps expert, professor Ali Karami from Baqiyatallah University, appeared on Iranian television and described coronavirus as a 'biological ethnic weapon' specifically created by the 'Americans and Zionist regime' to target Iranian DNA, which, Karami noted, explains the high coronavirus mortality rate in Iran. Professor Karami went further and said that Italy also suffers a high death rate since 'the genetics of the Italian people are very similar to the Iranian people'.

Another issue is racism and xenophobia. Since some bigots associate the virus with China, Chinese media has also initiated an anti-racist campaign to address xenophobia and racial prejudice. Even the New York Times and the Anti-Defamation League (ADL) addressed the emerging hatred of Chinese-Americans. As mentioned above, the Jews too are being targeted as the masterminds behind the virus for various delusional reasons such as controlling the world or dilution of populations.

## COVID-19 on the Dark Web: How Powers Can Spread Chaos and Dis/Misinformation

Internet users perceive online information to be just as authentic as television news and rarely verify the information they read online. Official press releases by governments are considered by some to be particularly unreliable as they are perceived to be driven by state interests. The rate of manipulation of online information has increased massively in recent years as information warfare became a common tool of state and non-state actors around the world.

This article examines the spread of dis/misinformation on the dark web and its adverse effects concerning the coronavirus, primarily on TOR, the most popular and accessible platform on the dark web. Many dark web users rely on the platform for information and are routinely exposed to dis/misinformation and to conspiracy theories. Dark web information consumers might not follow local instructions for quarantine and restrictions suggested by the World Health Organization (WHO) and their own governments, as they might think the measures are purposely misleading.

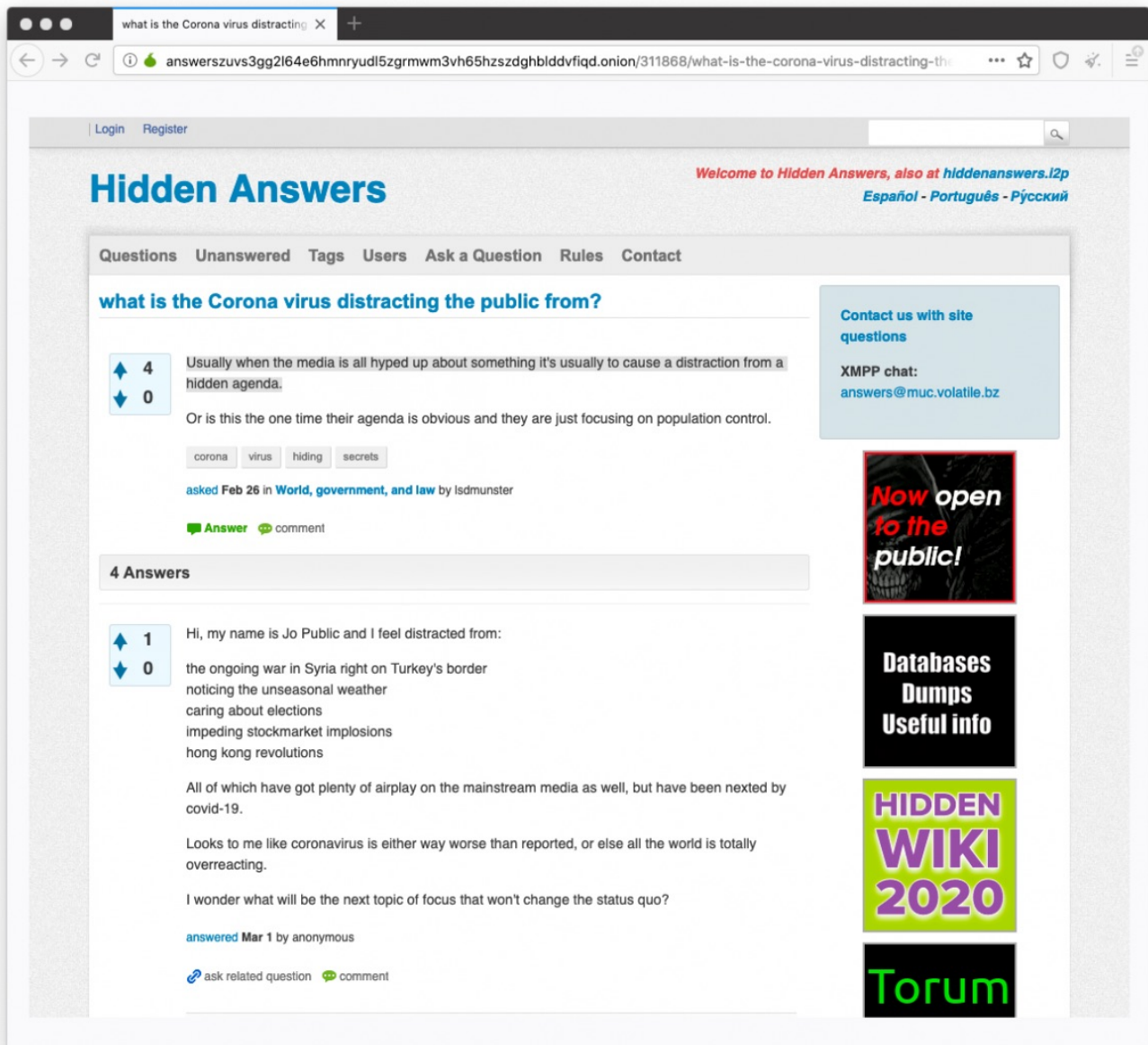
Some think, based on consumed dark web information, that the government or foreign forces engineered the virus for financial benefits, population dilution, balancing of global powers and other delusional reasons. The ones that have already believed conspiracy theories find the dark web information consolidating, further 'proof' for their conspiracies. The amount of dark web users is much smaller than the amount of surface web users, however, users can further traditionally spread the rumors to their social circles and publish it on social media or even on unreliable traditional media. The word then spreads from person to person.

## Dark Web Ethnography: Some Worrisome Examples

While exploring the dark web, most users will encounter popular search engines such as *Ahmia.fi* or *Torch* which will quickly lead them to online repositories such as the *HiddenWiki* since the DNSs (Domain Name System), IPs and ports on the dark web constantly change and are hard to remember.[1] On the popular forum and board of the conspiracies, *Neinchan*, the website administrators have opened up a special board just for the topic of the virus. Interestingly, some information was defaming China and other was defaming and blaming the US for the virus.

# Coronavirus Conspiracies and Dis/Misinformation on the Dark Web

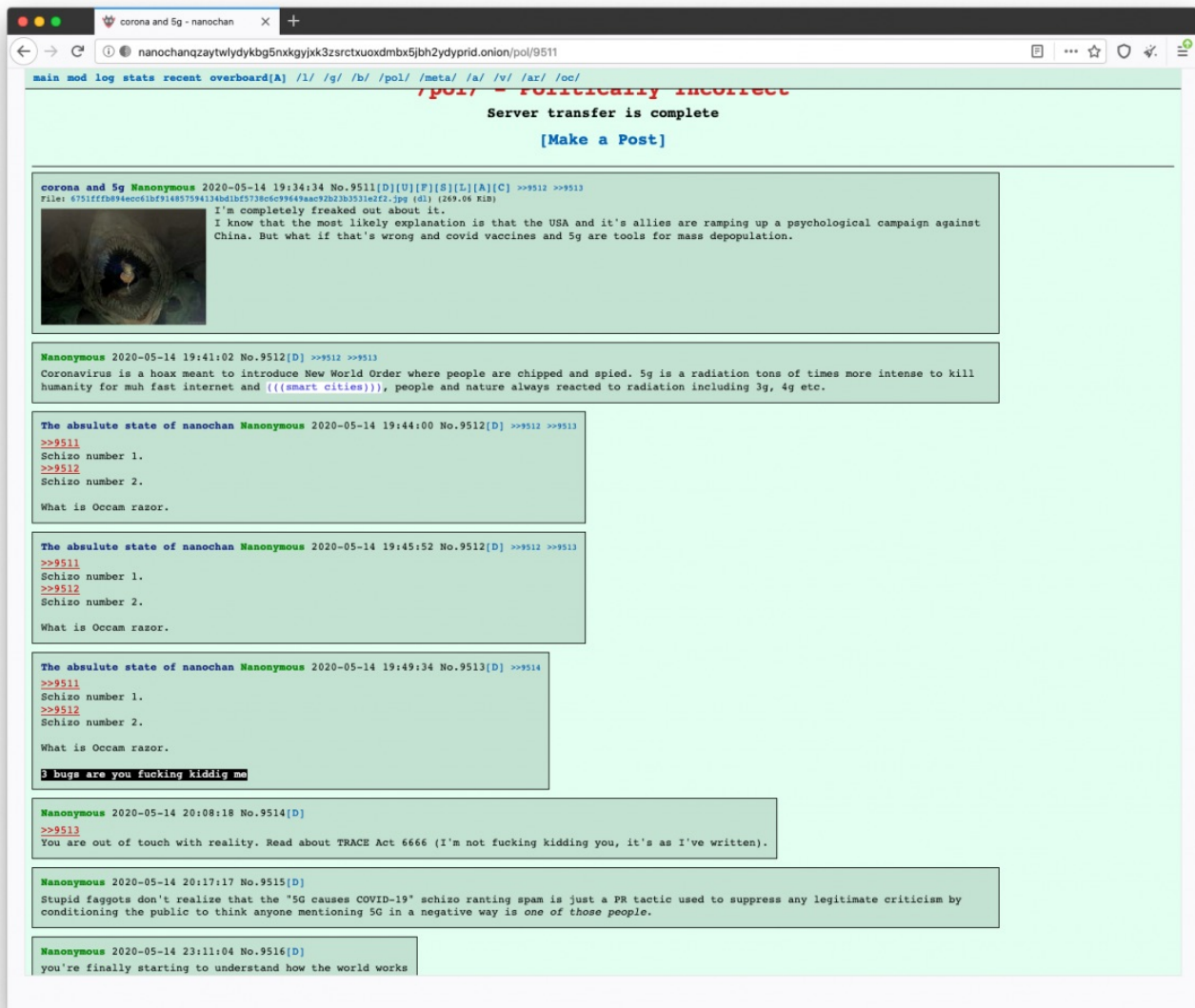
Written by Lev Topor and Pnina Shuker



In one of the most popular boards on the TOR dark web, *Hidden Answers*, anonymous users associated the virus to the US military, biological weapons and further global conspiracy. Some even assign the virus to the layout of 5G networks. One user asked, “what is the Corona virus distracting the public from?”, “Usually when the media is all hyped up about something it’s usually to cause a distraction from a hidden agenda”. On *Nano Chan* board an anonymous user wrote that the virus is “a hoax meant to introduce New World Order where people are chipped and spied.” In the *Nano Chan* board, the virus was vigorously associated with biological weapon development by the US. One user referred others to watch a video on the regular web, titled his post “COVID-19 and the DEEP STATE.” Another example is: “What if ... they all agreed to spread a bio-weapon to remove most of the elderly and remove the cost burden?”, “Governments in Europe encourage people to mingle in carnival while they had clear knowledge that this will spread the infection”. Further, while the dark web is known for drug markets, N95 Filter masks are being sold, emphasizing that they do not ship from China and that they are ‘clean’.

# Coronavirus Conspiracies and Dis/Misinformation on the Dark Web

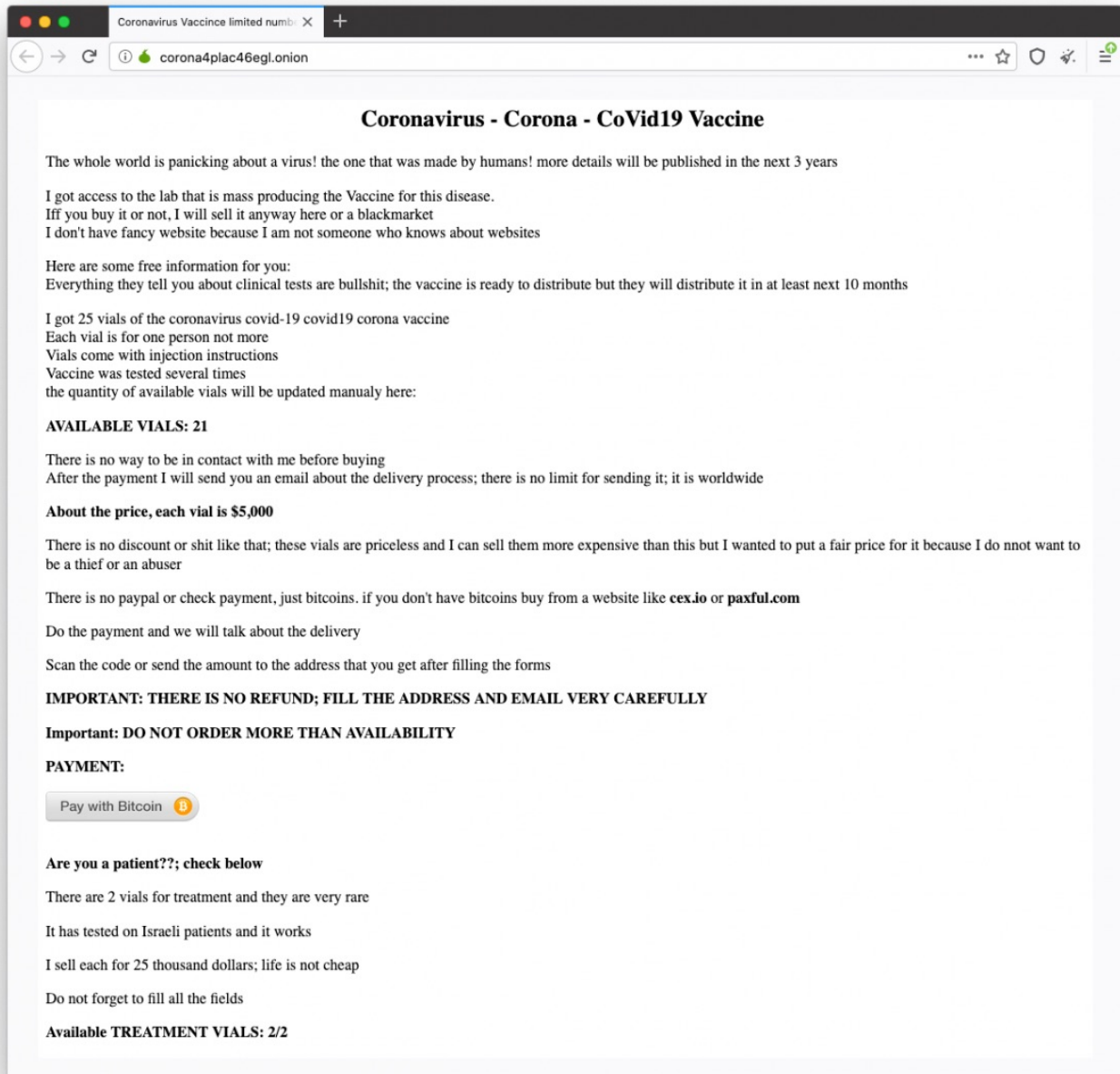
Written by Lev Topor and Pnina Shuker



People and governments worldwide are anticipating for a scientific breakthrough regarding vaccines. However, [fake] vaccines are also sold on the dark web, promising to cure people as the vaccines are presented as stolen/taken from the government, which, allegedly holds it. The false vaccines are not only dangerous because they are made from unknown and unregulated substances, they are also dangerous because consumers might think they will be immune and can then avoid local restrictions and social distancing. They can infect themselves but worse – they can infect others. These types of vaccines are mainly frauds and phishing attempts but they are also promoted by adversaries and propagandists.

# Coronavirus Conspiracies and Dis/Misinformation on the Dark Web

Written by Lev Topor and Pnina Shuker



## Conclusion

Throughout this article we examined the spread of dis/misinformation on the dark web, mainly on the TOR platform, about the Coronavirus pandemic. With the intensification and proliferation of information warfare between global powers as well as the spread of extreme conspiracy theories by white supremacists, terrorists and anti-authority propagandists, we argue that dark web Coronavirus information can be extremely dangerous as many internet users perceive it to be authentic and truer than official authority statements. This deepens the ongoing authority crisis even further. Our concern is that unreliable information can make the virus even more lethal as those who consume and believe it are more likely to disobey quarantine, restrictions and other regulations. Interestingly, as the dark web is used less in comparison to the regular web, our concern also regards in-direct, proxy, spread of information since people are more likely to believe information and stories they heard during more private and personal interactions with their peers, friends and family. It takes only one dark web user to 'infect' their peers. Thus, like the virus, this infodemic can also grow exponentially and multiply conspiracy believers, even though most were not exposed to the

# Coronavirus Conspiracies and Dis/Misinformation on the Dark Web

Written by Lev Topor and Pnina Shuker

actual source.

## Note

[1] That is the reason why we chose to place online screenshots instead of adding links.

---

## About the author:

**Dr. Lev Topor** is a Senior Research Fellow at the Center for Cyber Law and Policy at the University of Haifa, Israel and the Executive Director of a cyber and business research firm OTB Intelligence Ltd.

**Pnina Shuker** is a Neubauer research fellow at the Institute for National Security Studies and a PhD Candidate (ABD) at the Bar Ilan University, Israel.