DARKOWL

# PROJECT HOPE SUGGESTS NO HOPE FOR INTERNET FREEDOM IN RUSSIA

**LEAKED DOCUMENTS SUGGEST RUSSIA'S NEW RESTRICTIVE INTERNET LAW HAS BEEN IN THE WORKS FOR YEARS**

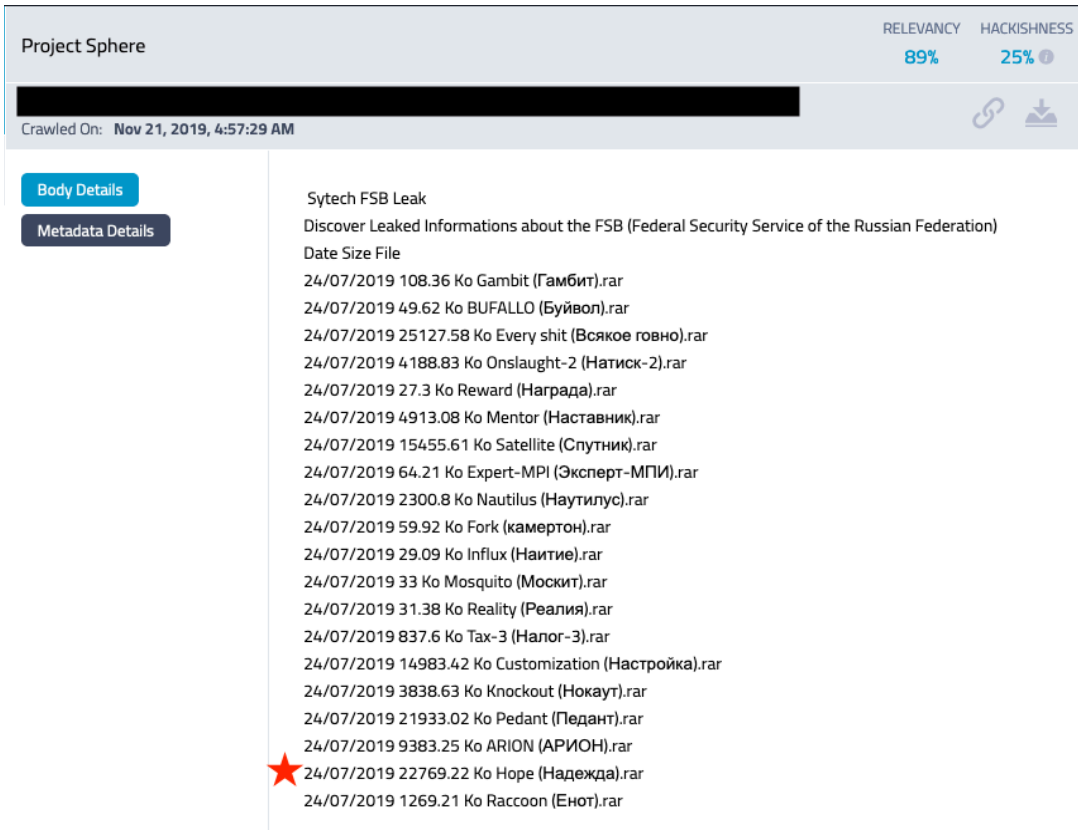
## INTRODUCTION

In July of 2019, 7.5 TB worth of documents that were stolen from a Russian FSB contractor known as SyTech were published on the darknet by the hacker group 0v1ru$. Included in the documents is a project known as "HOPE," which contains contents focused on how Russia intends to control the flow of information within and outside of their borders. While the notion and development of nation-wide intranets that exist in isolation from the global internet at the behest of nation-state authorities is nothing new (and in fact it has become increasingly common), it remains noteworthy – largely due to its association with politically oppressive regimes.

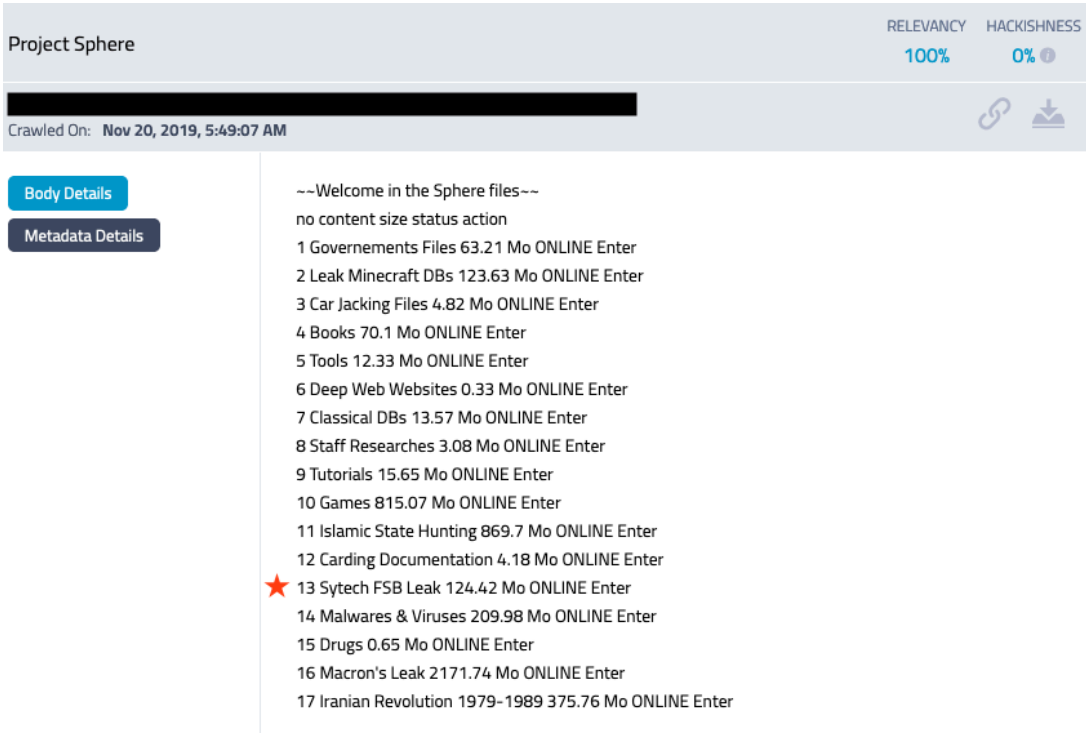
After discovering the leaked SyTech documents on DarkOwl Vision (pictured on Page 2), our analysts decided to take a closer look at project HOPE due to its relevancy to decentralized internets (including darknets). Upon conducting this analysis, DarkOwl researchers determined that Russia has been developing some of these plans as far back as 2012 and have concluded that it is very likely that HOPE was the foundation for Russia's new Sovereign Internet Law, which was recently enacted on November 1st, 2019.

### TABLE OF CONTENTS

# LEAKED DOCUMENTS FOUND IN DARKOWL VISION




*Images A and B: Screenshots from DarkOwl Vision showing the SyTech FSB leak freely available on the dark web*



# THE SYTECH LEAK

## WHO IS SYTECH?

SyTech was a Russian Federal Security Service (a.k.a. the FSB, the successor agency to the KGB) contractor registered in Moscow that primarily focused on electronic and signals intelligence research. Publicly disclosed customers of the FSB include the national satellite communications operator JSC RT Komm.ru and the analytical center of the judicial department under the Supreme Court of Russia. Other non-public projects were commissioned by military unit no. 71330, which is believed to be part of the 16th Directorate of the FSB - who were accused of sending files with spyware to Ukrainian military and intelligence agencies in March 2015. Ironically, SyTech is also located in the same building the 16th Directorate of the KGB of the USSR previously occupied. Their 2018 public contract value was 40 million rubles, or $622,631 USD.

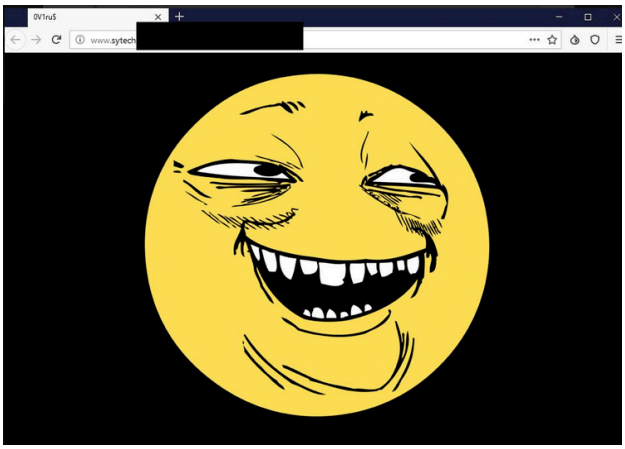


*Image C: The yoba-face icon displayed on SyTech's website*

## SYTECH HACKED

On July 13, 2019, SyTech suffered what BBC Russia called "possibly the largest data leak in the history of Russian intelligence services" when a group of hackers identified as 0v1ru$ gained access to an active directory server, stole 7.5TB of data, and defaced their webpage with a "yoba-face".

Though the image was first posted to 4chan in 2008, it is now most prominently associated with this breach, as evidenced by the spike on GoogleTrends (pictured below) on the date the hack was published. Analysis of screenshots posted by 0v1ru$ suggests that the tools used to gain access were ticketer.py, PSExec, and proxychains.

The leaked data includes 20 non-public IT projects ordered by Russian special services and departments. 0v1ru$ copied the data, deleted it from SyTech servers according to Twitter screenshots (pictured), and shared the documents with Digital Revolution, a separate (to our knowledge) hacking group who successfully breached Kvant Research Institute in 2018. Digital Revolution shared the documents with journalists, published screenshots of information on their Twitter - while mocking Russian officials - and the documents became widely available across the darknet.

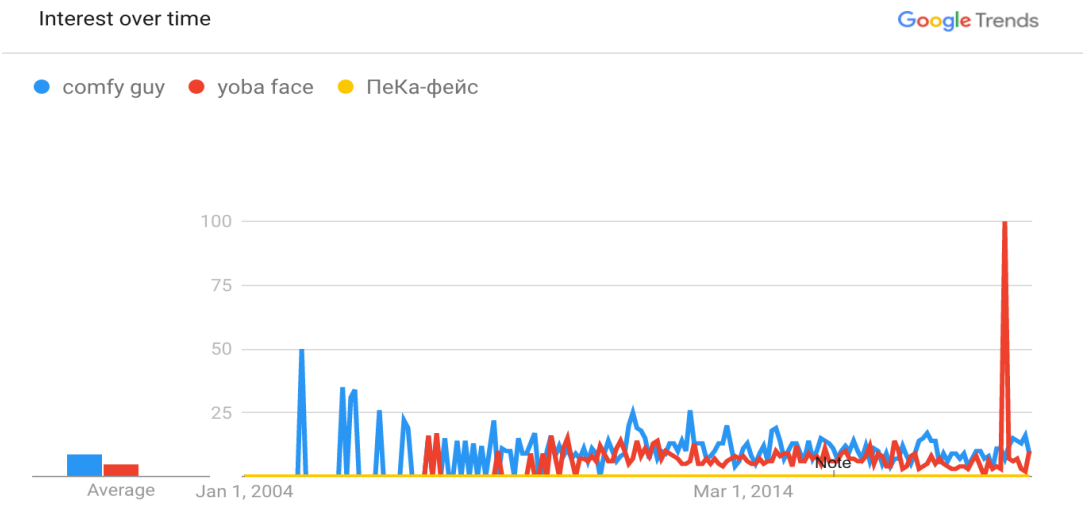
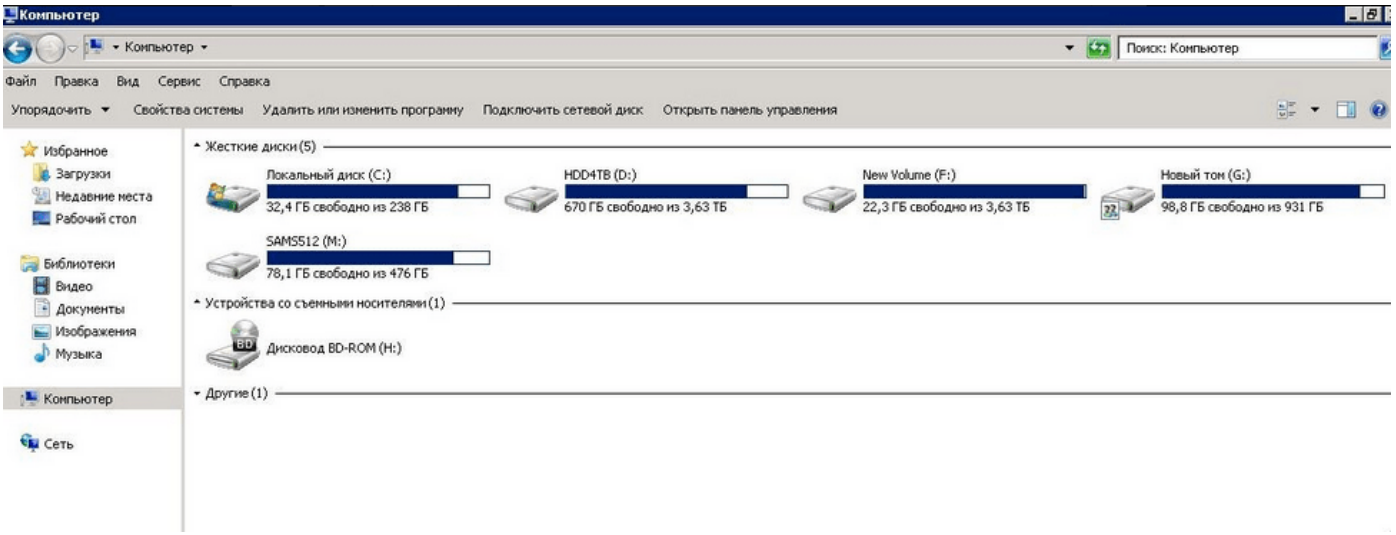



*Image D: Spike in interest in GoogleTrends*

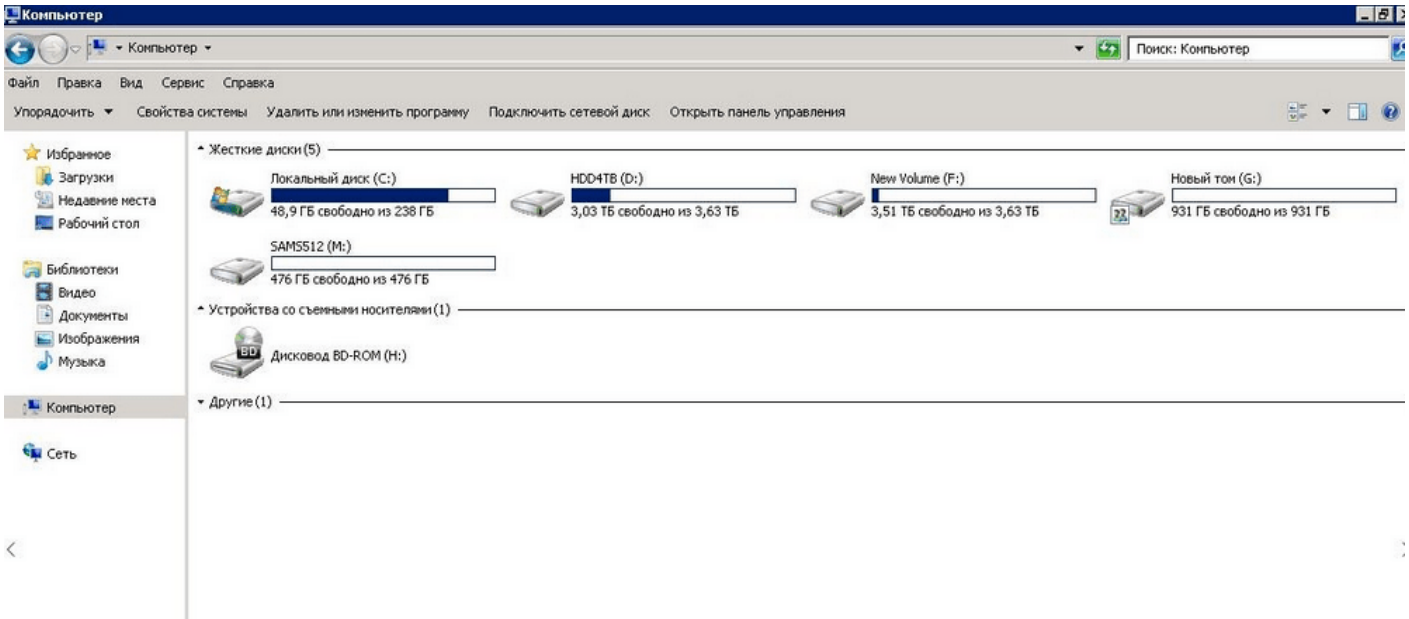
## Aftermath of the SyTech hack

0v1ru$'s Twitter account was deleted, and there has been no word from them since the day of the hack. It is unknown if they deleted their Twitter account or if Twitter removed the account. Their motive is unclear, though it seems the group was small in membership. Digital Revolution published a written piece encouraging dissent against Russian authorities in the wake of these documents in early August 2019, and have been silent since. SyTech's website has been offline since the defacement and no official statement regarding the hack or the future of SyTech was published. It is unclear if SyTech still exists, has been restructured, or dissolved after the leak.

There was no comment from the FSB, though BBC Russia reports no state secrets were leaked. Some have noted that this is another example of contractors being the weakest link in maintaining secrecy during research and development.




*Images E and F: Screenshots posted on Twitter by 0v1ru$ depicting SyTech servers before (above) and after (below) the documents in question were stolen*



# PROJECT HOPE

Though media widely reported on the SyTech hack itself, very few individuals or media outlets have examined the contents of the leaked documents. The level of detail, total amount of information, and potentially compromising information is not apparent from reading currently published reports; in most cases, a brief summary of a handful of the 20 projects is provided, and often, these summaries are not in English. DarkOwl analysts have obtained these documents and conducted analysis to:

1) **Examine the extent of leaked information – were only project summaries leaked, or entire proprietary technical plans?**

2) **Examine the impact of leaked information – did this leak impact or result in any legal or social issues in the future?**

3) **Examine the utility in analyzing leaked information – does the resources expended to acquire and analyze these documents produce actionable intel, open further lines of inquiry, or increase our knowledge base surrounding these issues?**

To accomplish these goals, DarkOwl analysts examined one of the twenty leaked projects: надежда, or Nadezhda, which translates in English to HOPE.

## WHAT IS PROJECT HOPE?

HOPE's main directive was to develop a method of disconnecting Russia from the global internet, while allowing information to still travel within Russia; in other words, they sought to develop their own nation-wide intranet. Purportedly, this would aid in protection from a foreign cyberattack - allowing Russian authorities to theoretically "unplug" Russia from the global internet to halt foreign attacks - if the technology developed via this project proved successful.

This work was carried out between April 1, 2013 and October 31, 2014 and was funded by Russia's military unit no. 71330.

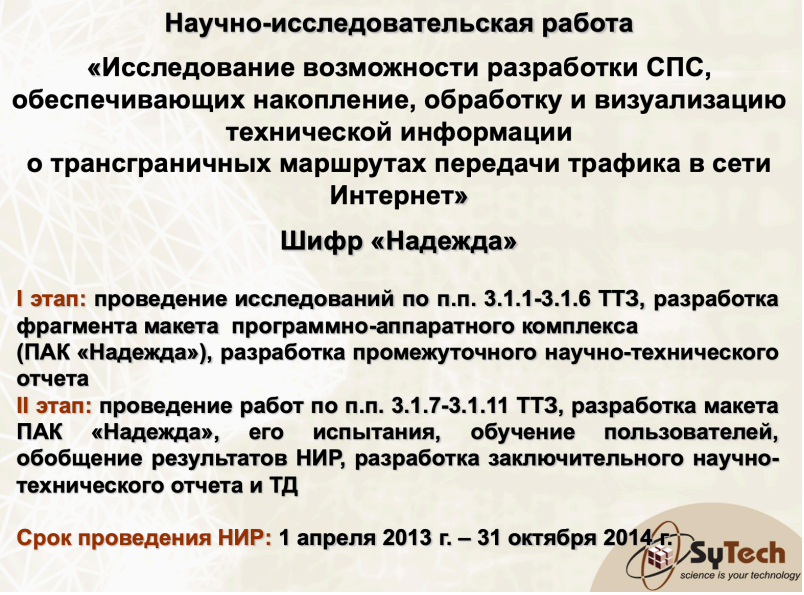



*Image G: Screenshot from SyTech PowerPoint indicating research goals and dates the research was conducted*

Once extracted, it was discovered that, unsurprisingly, the entire HOPE folder was in Russian. The folder contained 5 Microsoft Word documents, and a PowerPoint presentation. The bulk of the information from the documents was translated via Google Translate, though Russian translators assisted in the interpretation of potentially inaccurate or mistranslated words. One document in the leak indicates that it is likely all of these documents are components of a larger "Scientific and Technical Report" on the HOPE project, totaling 519 pages, 82 figures, 201 tables, 110 literature sources, and 7 appendices.

## THE CONTENT OF THE DOCUMENTS

The SyTech developed PowerPoint presentation appears to be a summary of the research and development conducted during the HOPE project. It is likely this was created near the end of the project in 2014 and presented to military unit no. 71330. It summarizes the work completed by SyTech, but also names and summarizes the work done by other collaborators on the HOPE project. According to this, the collaborators of HOPE are:

- **SyTech, who primarily focused on the visualization and analysis of cross-border routes for Internet traffic**
- **The RZNF Federal State Unitary Enterprise, who worked on a project codenamed "Nadezhda-T", aimed at monitoring and filtering traffic**
- **Institute for Security and Information Analysis, responsible for compiling the work done on HOPE and testing it and training future users**

The presentation also lists the sources of information they used, which are primarily in English and are publicly available. The results indicated success in achieving their research goals at a small scale but raises concerns about scalability.

The Word documents are components of a larger "Scientific and Technical Report" on the HOPE project, written at various stages in the project. One of the final documents suggest interim and final reports, thus there is some degree of overlap in the information included in these documents.

The first document is only 2 pages and seems to have been created at the genesis of the HOPE project. It was likely created in November or December of 2012 and states a generic goal of "studying the principles of cross border routing on the internet." It also states goals of examining vulnerabilities in TCP and Border Gateway Protocol (BGP), routing traffic through trusted government nodes, and the storage and analysis of traffic through these nodes.

All other documents are components of the Scientific and Technical Report at various stages in development. Two of these documents are highly technical examinations of topics such as traffic routing tests, BGP tests, and development of special visualization software

Of particular interest for this post is a 260-page document that indicates it is the final version of the Scientific and Technical Report. This appears to have been delivered to the customer at the same time the PowerPoint was created and delivered. It includes details such as:

- **The required software and OS**
- **Shared libraries**
- **Server platforms**
- **The inclusion of government connections.**

There is also some discussion of the use of deep packet inspection to analyze traffic, and criteria that may be used to filter and direct traffic. The report suggests that the research goals were met on a small scale; this includes the development of "state machines" provided to ISPs and includes diagrams of the machines and their functionality.

.


*Image H: Leaked PowerPoint slide demonstrating newly developed visualization capabilities*

## KEY TAKEAWAYS FROM THE PROJECT HOPE DOCUMENTS

These leaked documents show that SyTech and others were early in the development and testing phases of a project that was concerned with monitoring internet traffic, routing traffic based on state-developed criteria, and gaining control over internet access within the borders of Russia. In 2013-2014, when this project was underway, most work focused on what appears to be proof-of- concept/prototype development. To our knowledge, this was not tested on a larger scale, though the documents do indicate some concern over scalability. However, the PowerPoint indicated large-scale testing would be the responsibility of a non-SyTech body, thus, wouldn't be included in these leaked project files. It should be noted that involvement of other agencies in the HOPE project has not been reported in media reports to date.

Analysis of the technical documents suggest that control of internet traffic would be primarily accomplished by state sponsored BGP hijacking. A full analysis of this process is outside the scope of this post, but effectively, BGP hijacking uses the assumption that interconnected networks are telling the truth about which IP addresses they own to maliciously reroute internet traffic. In layman terms, it has been compared to changing out the exit signs on a stretch of freeway and rerouting traffic to incorrect exits, if no one were watching the freeway signs. BGP is managed by ISPs; considering the extensive research SyTech conducted into BGP traffic and the installation of technology at Russian ISPs, it is a strong possibility that BGP hijacking is the foundation for Russia's plans to control the internet.

Since HOPE was carried out, there has been a great amount of reporting and concern surrounding the development of Russia's nation-wide intranet. DarkOwl analysts believe it is likely that HOPE became the foundation for what is now known as Russia's Sovereign Internet Law.

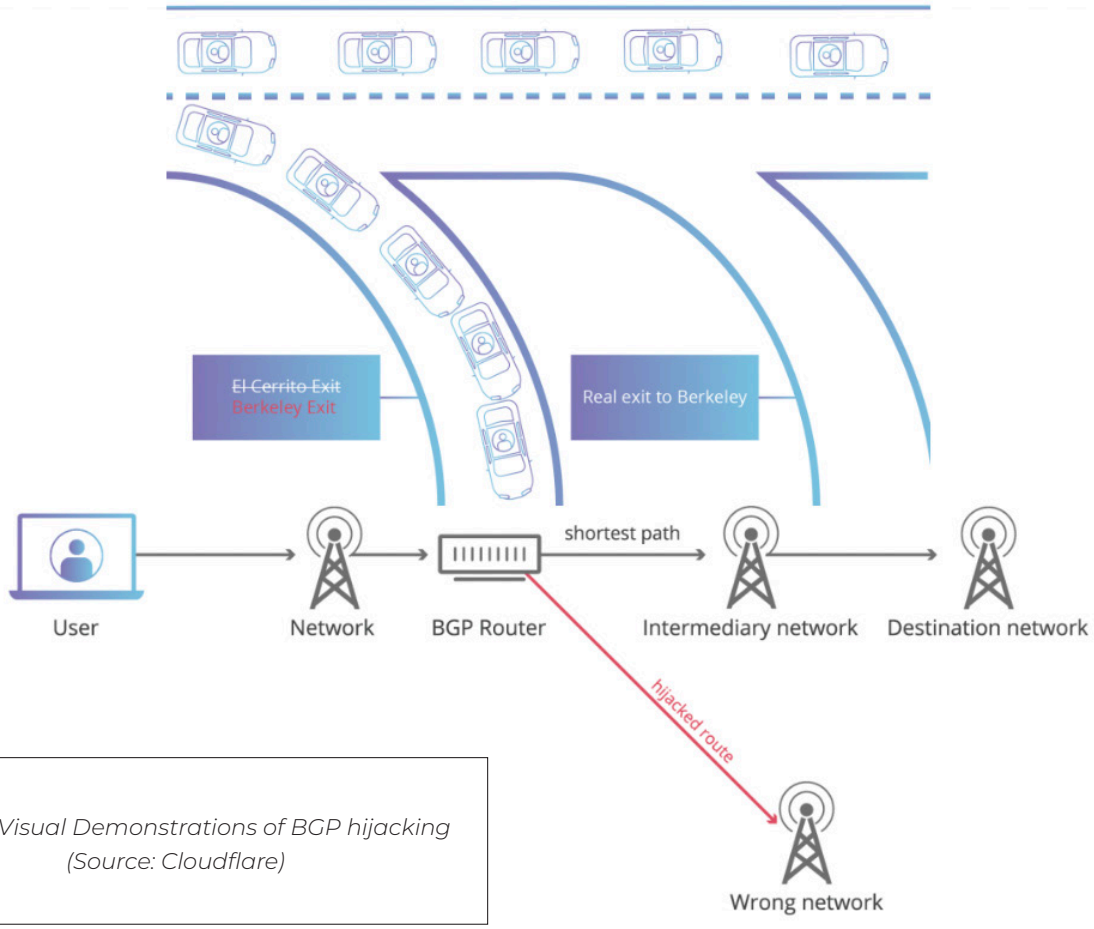



*Image I: Visual Demonstrations of BGP hijacking (Source: Cloudflare)*

# RUSSIA'S SOVEREIGN INTERNET LAW

On November 1, 2019, Russia's Sovereign Internet Law took effect, giving Russian government officials a higher degree of control over the nation's internet access and content. Ostensibly, the law is aimed to protect the nation's cybersecurity by allowing government officials to block access to content when an "emergency" has been declared.

In practice, the law has the largest impact on internet service providers located in Russia. Under this law, ISPs are required to:

1) **Install equipment that routes Russian internet traffic through state-controlled servers in the country**

2) **Install equipment capable of deep-packet inspection, which is capable of not only identifying the source of traffic but the filtration of content**

The first requirement is aimed at creating a new DNS system that can filter traffic in a way that data sent between Russians reaches its destination while any traffic directed towards foreign computers is discarded. Theoretically, this allows for Russia to essentially "unplug" from the global internet while nation-wide Runet service is uninterrupted. This is purportedly to protect Russia in the event of foreign cyberattacks or sanctions that attempt to isolate the country's internet presence; for example, when US Cyber Command cut off internet access to the infamous Kremlin-backed Internet Research Agency in efforts to defend the 2018 US Midterm Elections against foreign interference. Notably, this new DNS system is not expected to take effect until 2021.

The second requirement allows state regulators to filter traffic and block what it wants on a granular level; elements as small as individual social media and forum posts can be examined and blocked based on the content of the messaging. Deep packet inspection (DPI) technology is universally used by ISPs to prioritize traffic and block unwanted protocols; however, in this case, the traffic is not controlled by the ISPs but rather Russian communications regulator Roskomnadzor. The language surrounding this aspect of the law is, likely purposefully, vague; the law gives regulators full discretion to decide what constitutes a security threat or dissent that may harm the "stability, security, and integrity" of the internet. According to open source reporting, tests of Russian DPI technology will continue in the Urals region until the end of 2019.

## PUBLIC RECEPTION OF THE LAW

The degree to which the Russian government can control the flow of information due to this law has drawn strong reactions from both the Russian populace and international community.

According to research conducted by the Russian state-sponsored pollster, VTsIOM, 52% of Russians indicated they were opposed to the sovereign internet bill and the internet should play a role in "uniting the whole world", while only 23% believed the internet should be limited to the country's borders. Rallies opposing the bill in Moscow, Voronezh, and Khabarovsk were "some of the biggest protests" in years, totaling over 15,000 people in Moscow alone (though police estimated only 6500 attendees). The law has often been referred to as a digital Iron Curtain, harkening back to the Cold War separation of the USSR and the West.

Outside of Russia, the law has been almost universally condemned. Ten human rights, media, and Internet freedom organizations released a joint statement criticizing the law and calling on President Putin to not sign it - though he did one week after publication of the statement. They and others suggest that the law does not satisfactorily define what constitutes security threats and appropriate responses and lends the government too much discretion in how these laws will be enforced. There are also no legal protections for internet users to prevent ISPs from accessing, collecting, and selling the information gleaned via DPI. Many view this new law as continuing the erosion of internet freedoms in Russia; Freedom House categorizes Russia as "Not Free" and argues internet freedom is continuing to decline because of this law and other policies. For instance, according to a report from the Agora International Human Rights Group, someone in Russia was imprisoned for their online activities every 8 days in 2017.


*Image J: Russian Protests against the Sovereign Internet Law (Source: Associated Press)*

Moving beyond criticisms based in human rights and social issues surrounding the law, numerous technical experts are skeptical that enforcement of the law is currently possible. Both the establishment of a nation-wide intranet and DPI inspection of all traffic faces numerous, possibly insurmountable, technical hurdles.

Many experts are quick to point out that the Russian development of their alternate DNS system is dissimilar to China's Great Firewall; whereas China's internet was developed via a small number of state-run network operators - with a goal of restricting access in mind - Russia's internet has developed freely over the last 30 years. Undoing that development would be a monumental task; the more developed a country's infrastructure, the more laborious the blackout procedure becomes. David Belson, the senior director of Internet Research and Analysis at Internet Society, told NPR:

> *"..there were dozens of existing internet exchange points in Russia, some of which have hundreds of participants... basically its challenging - if not impossible, I think – to completely isolate the Russian Internet."*

Twelve organizations oversee the root servers for the current DNS system; zero of these are located in Russia. Undoing those global network connections will be difficult, and this kind of regulatory model could risk damaging the reliability of internet connections in Russia. According to Sophos:

> *"Internet traffic isn't like a pipe that can be turned on and off or diverted at will. It functions as a cooperative system in which Russian ISPs must peer traffic that is heading to other destinations in ways that belie simple concepts of internal and external, good and bad."*

Some predict that, if nation-wide separation from the global internet proves impossible, it will be more likely that specific regions within the country can be disconnected for short periods of time.

Previous attempts at using law to forbid a form of technology has failed; last year, Russia attempted to ban the messaging app Telegram for refusing to provide encryption keys to Russian authority, to practically no effect, other than simultaneously blocking access to allowed content. Experts also point out that the rhetoric surrounding this bill regards protection from foreign cyberattacks, yet the DPI requirement of the law only serves to increase control of internet within Russia. Law-abiding users will notice the change; the installation of DPI equipment across all ISPs in Russia has been compared to the crush of passengers trying to get on the Moscow metro at rush hour.

There is no consensus among experts what impact this law will have long-term; it may lead to the types of humans rights violations watchdogs are worried about, or it could cause no change at all. It is also uncertain how this law may impact Russian darknet activity, even among Russian darknet users (Figure 8). Activity may increase as users seek to circumvent the newly enacted law; it may decrease if the technology implemented is sophisticated enough to limit dark web activity. Theoretically, BGP hijacking could manipulate and control entry relay node traffic which would destroy the anonymity provided by Tor for Russian users.

Russia has a sizable presence on the dark web and is the most common foreign language in DarkOwl's database; DarkOwl will continue to monitor this activity for any changes or modifications of dark web use.

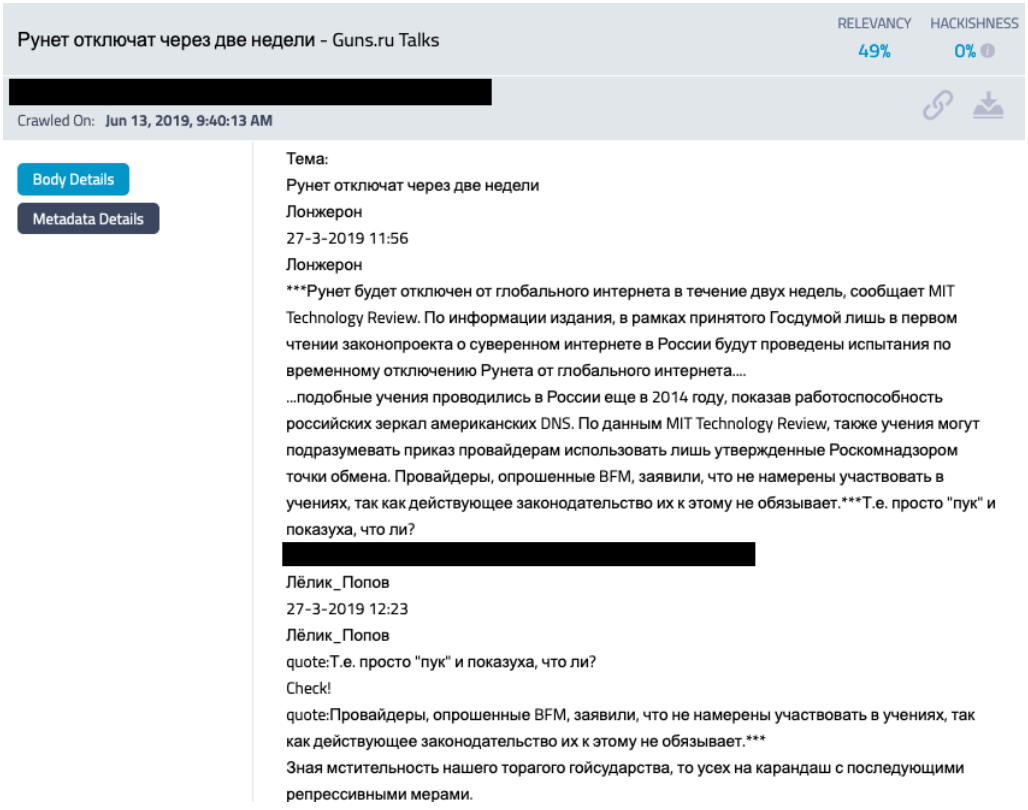



*Image K: Screenshot from DarkOwl Vision displaying Russian forum discussion of the Sovereign Internet Law*

# CONCLUSIONS

Upon revisiting the questions we sought to answer during our analysis of the leaked documents, we were able to come to several conclusions:

1) **Were only project summaries leaked, or entire proprietary technical plans?**

Hackers leaked extensive documentation surrounding the HOPE project on the dark web. The leak included project summaries, supporting technical documents, test results, and the final customer product. It is clear there was much more leaked than what was reported via most media sources and raises numerous questions over what is contained in the leaks of other projects from SyTech.

2) **Did this leak impact or result in any legal or social issues in the future?**

Although it cannot be directly linked, the preponderance of evidence suggests that HOPE was a precursor to the Russia Sovereign Internet Law. The stated goals and methods discussed in HOPE directly reflect the realities of the Sovereign Internet Law. Though the official response minimized the impact of these leaks, the documents demonstrate a clear connection to future legal and social developments.

3) **Does the resources expended to acquire and analyze these documents produce actionable intel, open further lines of inquiry, or increase our knowledge base surrounding these issues?**

The examination of these documents provided insights unavailable in any other report or analysis of the SyTech hack. Considering the information obtained and that HOPE likely resulted in a divisive law, future research should be conducted on the other leaked documents in efforts to predict other future policy or technological development.

## THE INTERNET AS A HUMAN RIGHTS ISSUE

The United Nations Human Rights Council (UNHRC) has consistently stressed the importance of taking a human rights based approach to internet access. In June of 2016, the UNHRC passed resolution A/HRC/38/L.20, addressing "the promotion, protection, and enjoyment of human rights on the internet." The resolution affirms that the "same rights people have offline must be protected online," and outlines the perceived importance of internet access to the human rights protections of the citizens of member nations.

Press coverage of the initiative reported that, despite passing with consensus, Russia and China opposed this resolution and sought


*Image L: United Nations Human Rights logo*

## THE INTERNET AS A HUMAN RIGHTS ISSUE (CONT.)

to remove language relating to the "human-rights based approach" to internet access. This is relatively unsurprising; China's "Great Firewall" stratagem to internet censorship is well-documented by academics, human rights watchdogs, and western media. Furthermore, the notion of free access and usage of the internet has been under attack by various nation-states, as reports of government-backed nationwide internet outages, social media blackouts during military conflict, the criminalization of dissent, and the murder of bloggers and journalists have only increased in the public eye since the passing of this resolution.

The UNHRC further demonstrated this commitment to internet freedom in July of 2018 when they reaffirmed the internet protection resolution - with no States formally dissociating from the language in the resolution. However, the emphasis on protecting human rights online as well as offline is minimized in this resolution, and the United States no longer is listed as a participating State.

Further developments have shown no signs of Russia slowing down in their pursuit of state-controlled internet, often hiding behind a veil of curbing cybercrime. Other nations such as Iran have followed suit and have begun exercising control over internet access.

## WILL THESE NEW RESTRICTIONS LEAD TO AN INCREASE IN DARK WEB USERSHIP?

In name, the Russian Sovereign Internet Law is already in effect. However, the social impact from this law will not be felt until later, and it is uncertain how this law will alter the amount and type of activity on the dark web, if at all.

Fundamental changes in the structure of the internet don't occur overnight, or over just a few years – research, development, and implementation of this technology took nearly a decade via the HOPE project, and still isn't close to completion. If we want to see what is coming next, it may be best to look at similar projects that are being researched now rather than wait for their deployment.

## REFERENCES

Fortuna, Andrea. 2019. The SyTech Hack: a brief screenshot-based attack analysis. https://www.andreafortuna.org/2019/07/21/the-sytech-hack-a-brief-screenshot-based-attack-analysis/

Associated Press. 2019. New Russian Internet Law Stokes Censorship Fears. https://www.usnews.com/news/world/articles/2019-05-01/new-russian-internet-law-stokes-censorship-fears

Holt, Kris. 2019. Russian 'sovereign internet' bill could give Putin his own Great Firewall. https://www.engadget.com/2019/03/05/russia-internet-bill-great-firewall/

Nakashima, Ellen. 2019. U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

Dunn, John. 2019. Russia's sovereign internet law comes into force. https://nakedsecurity.sophos.com/2019/11/04/russias-sovereign-internet-law-comes-into-force/

Ivanko, Igor. 2019. Majority of Russians Oppose 'Sovereign Internet' Bill – Poll. https://www.themoscowtimes.com/2019/04/29/majority-of-russians-oppose-sovereign-internet-bill-study-a65419

Hamraev, Victor. 2019. Digital times have come in Russia. https://www.kommersant.ru/doc/3960049

Ingber, Sasha. 2019. Russians, Fearing Internet Isolation, Protest Government Plan. https://www.npr.org/2019/03/11/702347714/russians-fearing-internet-isolation-protest-government-plan

Vasilyeva, Maria. 2019. Thousands of Russians protest against internet restrictions. https://www.reuters.com/article/us-russia-internet-protests/thousands-of-russians-protest-against-internet-restrictions-idUSKBN1QR0HI

Economy, Elizabeth. 2018. The great firewall of China: Xi Jinping's internet shutdown. https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

Feldstein, Steven. 2019. To end mass protests, Sudan has cut off Internet access nationwide. Here's why. https://www.washingtonpost.com/politics/2019/06/13/end-mass-protests-sudan-has-cut-off-internet-access-nationwide-heres-why/

Martineau, Paris. 2019. Turkish ISP Blocks Social Media Sites Near Syrian Border. https://www.wired.com/story/turkish-isp-blocks-social-media-syrian-border/

Boyle, Emma. 2016. UN DECLARES ONLINE FREEDOM TO BE A HUMAN RIGHT THAT MUST BE PROTECTED. https://www.independent.co.uk/life-style/gadgets-and-tech/un-declares-online-freedom-to-be-a-human-right-that-must-be-protected-a7120186.html

Human Rights Watch. 2019. Joint Statement on Russia's "Sovereign Internet Bill" https://www.hrw.org/news/2019/04/24/joint-statement-russias-sovereign-internet-bill

Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements. 2018. https://intelligence.house.gov/social-media-content/