allot
See. Control. Secure.

Position Paper

The Use of Digital Enforcement in Light of COVID-19

May 2020

Contents

Introduction

The continuous development of the Internet, its ever-growing number of users and virtually unlimited content sharing opportunities, inevitably raise the issue of legal Internet regulation and enforcement. With the Coronavirus pandemic, some of these challenges have become unbearable. All the uncontrolled illegal digital activities such as terrorism, drug trafficking and child pornography, have reached a level that calls for intervention. Law enforcement agencies have been forced to recognize the urgency of implementing digital enforcement as a means to prevent these activities. This can be achieved using more progressive tools that are currently being discussed or tested to deliver more advanced digital enforcement capabilities.

The current COVID-19 pandemic has led us to the inevitable limitation of our basic freedoms and rights such as movement, privacy and religion. Most of the world's governments have declared a state of emergency, allowing unprecedented measures in the name of public safety. More than ever, the digital world is a source of information for the masses and provides visuals to people who cannot leave their homes or debate the information coming from conventional sources.

The urgent need for continuous, detailed intelligence and insight from affected areas has forced massive usage of strategic tools already in place at law enforcement agencies (LEA). These tools that are commonly used to track criminals, terrorists or other governmental targets are now tracking citizens suspected of potentially carrying the COVID-19 virus.

Going forward, probably the most significant legacy of the Pandemic will be a major disruption of the intelligence world and the subsequent rise and democratization of massive digital enforcement and surveillance tools. This is comparable to the race for intelligence after the September 11 attacks.

Part I
Within the digital world

Cyberspace is not beyond the rule of law. The common standard for regulating digital space is to prevent social turmoil and division, but mainly to curb the spread of illegal content and extremist incitement. Although certain achievements in regulating the digital space have been made, recent events are bringing up unique and more severe challenges from many different sources that need to be addressed. Frankly speaking, we are all beginners in Digital Regulation and Enforcement. Furthermore, laws must be improved constantly to better regulate and control the digital world.

A report titled *Freedom on the Net 2018: The Rise of Digital Authoritarianism* released by Freedom House, a US-based NGO that conducts research on political freedom and human rights, notes that, ''In 2018 only, more than 17 countries approved or proposed laws that would restrict online media in the name of fighting 'fake news' and online manipulation.''

The report also shows that stricter Internet regulation will be an irresistible trend worldwide. More idealistic opinion makers claim that the power of the Internet can only be curbed by society itself without regulation by the state. However, we argue that the Internet without regulation will be like a lawless country, doomed to be filled with violence, hate and chaos. No country in the world can truly realize absolute freedom of speech in cyberspace. Without question, the pandemic, and events like it will be an accelerator for such results.

Another report from March 2019 by the Pew Research Center titled *For Local News, Americans Embrace Digital but Still Want Strong Community Connection*, analyzes the different channels through which Americans are receiving and collecting news and information. The report states that 89% of Americans get at least some local news digitally and about four-in-ten (41%) do so often. 12% of Americans often get local news from online forums meaning digital word to mouth. Another 15% get their news primarily from social media and 23% from news Websites. finally, 32% describe Internet as the most important way to get news. According to the report,

> *''The digital environment is now a key component in how Americans learn about local events and issues in the news. Today, almost as many U.S. adults say they prefer to get their local news through the Internet as prefer to do so through the television set.''*

At the time that this article is being written, the Coronavirus pandemic has already claimed 230,000 victims. But the worst seems yet to come. Our incapacity to foresee when humanity can take back control of a situation is generating an astronomic amount of discussion in online forums and alternative news sites.

And as if the pandemic itself was not enough, reports from South Korea are now mentioning reactivation of the Virus on cured patients. Our economies are being devastated and most of the world is maintaining full lockdown. The lack of visibility is leading state leaders to extreme and unprecedented measures.

Part II
Digital Enforcement During the Covis-19

We are presently witnessing one of the certain legacies of the coronavirus: Massive State digital Surveillance and Enforcement. Countries such as France, Germany, Israel, USA and the United Kingdom have unleashed their Intelligence and Law enforcement agencies with the hope that by controlling the crowd they may be able to control the virus.

Looking East toward the Asian countries, their strategies have solidified the decision to introduce massive digital surveillance and enforcement. South Korea and China made use of expansive and intrusive Digital Surveillance and Digital Enforcement technologies, enabling the successful control and recovery of the pandemic.

The digital technologies used to fight COVID-19 were made possible by shifting the control and traffic of national networks from telecom providers to the Government itself. For example, by modifying the prioritization of Internet network traffic from regular services to intelligence needs, states can generate sufficient bandwidth and redirect the traffic of all the digital Sources. Data from CCTV surveillance, credit card information, facial recognition, Internet surveillance, GSM and IP-based geolocation, and others are now rapidly and securely collected.

The collection and analysis of this monumental amount of data is also creating the necessity for securing the network and the new sources from third party threats.

Network security solutions are an important element of the mission as they secure any end points and the transit from the sources to the command and control center. LEA are capable of sealing the intelligence pipe without accessing the sources.

Finally, application control capabilities allow LEA to ensure the accuracy of the content available online and in forums aligned with the crisis management requirements. Anyone who tries to negatively influence the progress in the fight against the pandemic can be rejected from the network and rendered incapable of spreading their dangerous intentions. In extreme times, extreme measures are necessary.

Though some question if the ends justify the means, digital surveillance and enforcement have resulted in a lower death rate, faster recovery and reduced impact on local economies for the states who managed to make proper use of it.

Conclusion

It is evident that digital prediction and intelligence could help the world to better manage the next crisis whether it is a new pandemic or another event that we cannot yet foresee. The necessity and value of Digital Intelligence and digital prediction are unmistakable.

Networks have a very central role in our day to day lives; They are critical for most of our basic needs and essential for all national and international infrastructures. Even so, the infrastructures and services are predominantly managed by private companies whose priority and focus are purely financial.

Governments have a set of tools to monitor and control the networks via laws, regulations and political decisions. But there is too much exposure in the digital world and not enough ways to monitor and protect it.

The evident conflict between total visibility and privacy is making this challenge even more complicated. It is a shared responsibility between states and vendors to ensure the right expectations are set and that their available capabilities are optimally employed.