Legal Protest and Distributed Denial of Service

Joshua I. James*

March 26, 2013

1 Digital Protest

The United States government, via the "We the People" portal (petitions.whitehouse.gov), was petitioned by Dylan K. [1] to "Make, distributed denial-of-service (DDoS), a legal form of protest". The petition states that:

> *With the advance in [Internet technology], comes new grounds for protesting. Distributed denial-of-service (DDoS), is not any form of hacking in any way. It is the equivalent of repeatedly hitting the refresh button on a web page. It is, in that way, no different than any "occupy" protest. Instead of a group of people standing outside a building to occupy the area, they are having their computer occupy a website to slow (or deny) service of that particular website for a short time...*

The petition hits on a number of topics that are currently not well defined in terms of a 'physical reality', let alone a 'digital reality'. This work will attempt to examine different concepts proposed within the petition (as we interpret them), and informally compare such concepts to existing legislation. Note, this work should be considered merely as points for discussion, not academic definition or legal advice.

First, let's begin by defining what each part of the petition means. The first sentence could be taken to mean that Internet technologies have provided new ways to communicate and interact that has enabled the creation of new social groups with their own unique beliefs and cultures (cyber cultures). Further, these cyber cultures should have the same rights as those afforded in the physical world (i.e. in the U.S.), and thus be able to protest when those rights have been denied.

The second and third sentences propose that Distributed Denial-of-Service is not inherently hacking, but instead sending data, as intended, over a public network to a publicly accessible host.

The fourth sentence proposes that intentionally accessing a publicly accessible Internet resource is similar to assembling at a publicly accessible space in physical reality.

The final sentence proposes that having a group of people collectively access a publicly accessible Internet resource (digital space) with the intention of slowing or denying access to other users is equivalent to a group of people assembling in a public physical space.

2 Rights of Cyber Cultures

There are a growing number of works dealing with the definition, evolution and understanding of cyber cultures [2, 3]. Effectively, the proposed claim is that cyber cultures should be afforded the same rights that citizens enjoy in physical reality. The assumption in this case is that these rights are as defined by legislation in the United States.

Herein lies the first challenge: jurisdiction. Under what circumstances should rights to citizens on the Internet (netizens) be extended, and to what extent? For example, assume a cyber culture exists within an online Internet game. If the server for the game is hosted in the U.S., and the netizens that make up the cyber culture are U.S. citizens in physical reality, then their rights in physical reality should extend to digital reality since the digital reality is a media in which he or she is exercising their freedom of expression, etc. These freedoms may be limited by the policies of the game, but rights should be extended nonetheless.

Alternatively, if the game is hosted in a server that is physically located in China, and a U.S. citizen accesses the game from the U.S., there would not likely be any expectation of the U.S. citizen's physical reality rights (as protected in the U.S.) to be extended to the digital reality geographically hosted in China.

By considering rights of citizens based on jurisdiction, countries may begin to assign rights to netizens in a digital reality similar to the way that rights are protected in that country's physical reality. Essentially, a netizen that is from the host country is afforded the same rights (or lack of) they enjoy as a local citizen. A netizen that is from another country may be afforded the same rights (and restrictions) as an immigrant to that country.

Instead of considering dividing the Internet up by jurisdiction, this work will assume that rights as defined by the Universal Declaration of Human Rights (UDHR) [4] – Article 20 – are also extended to netizens in digital reality. This claim also appears to be held by, then Secretary of State, Hillary Clinton, who said, "The freedom to assemble and associate is applicable to cyberspace" [5]. The author presumes this right is extended to all netizens. When basic rights are guaranteed for all netizens regardless of geographic location, jurisdiction becomes (slightly) less of an issue.

*Digital Forensic Investigation Research Group (DigitalFIRE), University College Dublin, Belfield, Dublin 4, Ireland

3 The Legality of Distributed Denial of Service

For a definition of hacking, we can look at the U.S. Computer Fraud and Abuse Act [6]. In this act, many sections explicitly state that a system must be 'accessed'. As access is defined, however, it seems to imply gaining access into a system, e.g. gaining rights to a system through authentication or exploitation. Further, protected systems are defined, such as financial and critical communication systems, which are explicitly protected from any form of tampering.

Section 5A, however, says: "[Whoever] knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer... shall be punished". Further, the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information. The argument could be made that DDoS is the intentional transmission of information/code that impairs the availability of data. By this standard, DDoS should be considered illegal.

In this case the transmission of data with malicious intent may be illegal, while the transmission of the same data with non-malicious intent may not be illegal. Since intent of the transmission of data is being considered, so too could data transmission with the intent to protest. This work will assume that the intentions behind protesting are non-malicious, and the intentions of sending data is not with malicious intent, but instead with the intent to convey a message protected under UDHR Article 19, which states that everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

4 Public Spaces in a Digital Reality

The next question is whether visiting a publicly accessible website is like visiting a public space. Webster's Online Dictionary defines a public space as a place where anyone has a right to come without being excluded because of economic or social conditions. Indeed, any person can walk on a sidewalk, which is generally considered a public space. And from the public space a person may look at or into private property, with certain restrictions.

The online parallel could be that the Internet is a series of sidewalks that lead to a house. A website's landing page would be the exterior of the house. In more technical terms, making an HTTP request to the web host for the landing page would be like observing the house from the sidewalk. Arguably, if a user does not need to authenticate to access the landing page, then making a request of the server would be similar to walking down a sidewalk and observing a house. The question is, is making a request for a public web page similar to observing a building from a public space?

In this work it will be assumed that the Internet is a public space, and each server (website) is similar to a building. Passers-by may observe the house (server), either intentionally or not, as a consequence of it being connected to the public space. If, however, the user attempts to enter the server/website, they are then entering a private space. With this assumption, making a valid request for public information from a server should be considered as making a request (or an observation) from a public space. If the request can be made from a public space, then, as previously described, netizens should have the right to assemble on this public space.

5 Right to DDoS

The final question addressed in this work is whether assembly on a public space with the express intention of slowing to denying access is a legal form of protest. To answer this question, first we must look at how protest is defined. Specifically, (in our opinion) the petition sounds analogous to a picket line.

Picketing is a form of protest in which a person or group of people attempt to dissuade or prevent workers or customers from entering a business or other location. In many countries there is no explicit "right to picket", but peaceful protest is normally accepted under the right to assembly, with some restrictions. In the United Kingdom, "[t]he only purposes of picketing declared lawful in statute are peacefully obtaining and communicating information, and peacefully persuading a person to work or not to work" [7]. In many countries picketing is generally accepted as legal if the following conditions are met:

1. Local laws are followed, and police are obeyed
2. Local authorities are pre-notified
3. Picketing is done only on public property, or private property with permission
4. Entrances to businesses are not blocked
5. Employees and/or customers are not harassed
   (a) Should not restrict the rights and movements of other people
   (b) Non-violent

Violence in this case will be defined as rough or injurious physical force, action, or treatment; an unjust or unwarranted exertion of force or power, as against rights or laws. Harassment will be defined as to disturb persistently; bother continually; pester; persecute.

At this point, this work will need to make another assumption. Namely, that a botnet *legally* exists. For the sake of brevity, a legal botnet will be defined as one where all nodes are knowingly part of the network, and actively agreed to have their resources used for the collective purpose. While DDoS may not explicitly be hacking, computers infected with viruses are commonly used to commit DDoS attacks. In this case if a botnet is created through illegal means, then the action should also be considered illegal (regardless of overall intent). The assumption is that a collective of protesters are willingly donating their computing resources for the purpose of slowing or denying some service.

Assume that a botnet legally exists, the computing resources collectively assemble on a target public space with the purpose of protesting, and authorities were notified of the 'protest' ahead of time. According to the general rules for legal protest as given, there are still a number of challenges. First and foremost, entrances to businesses should not be blocked. In terms of DDoS, if sustained denial of service takes place, then access (entrance) to the server (business) is effectively blocked. This means that, at a minimum, sustained denial of service should be considered as a non-legal approach to protesting.

Next, we can consider denial of service that is not sustained. For example, if DDoS occurs every 10 minutes and is sustained for 30 seconds. This approach would result in degraded service, but not a complete denial of service. The challenge here comes from the definition of harassment. If a user (customer) were attempting to use a service, non-sustained denial of service would repeatedly affect that user's ability to use the service, but not block access to the service. This could be compared to continually, and forcefully, hindering the customer from accessing a business. Indeed, many Internet users may define dropped service connections to be disturbing, intentional or otherwise. In other words, intentionally and repeatedly affecting the user's connection could be considered harassment.

The final, and potentially most important factor is that DDoS does not explicitly communicate information. Picketers in physical reality can carry signs, handouts and have conversations to let the public and the companies understand why the group is picketing. The reasons for DDoS protests may be published somewhere, but there is little guarantee that the business – let alone the customers – would be able to determine why degradation of service was happening, and how to differentiate a protest DDoS from a non-protest attack. This is somewhat similar to a group of protesters congregating in front of a business, and without giving any reason, randomly restricting customers from entering. Protest should involve communication, and with DDoS communication to both the protested organization and its customers is not guaranteed.

6 Conclusions

By extending the UDHR to apply to all netizens, the right to assembly and right to expression online would allow protesters to congregate on a public space, which, we believe, can be defined as a publicly-accessible IP address. The result of this assembly may naturally result in degraded or even a denial of service to other customers. However, if the intention of the assembly is to degrade or deny service to customers, then the protesters have chosen to use threat to the business, and harassment of it's customers as its form of protest. In our opinion, protest should (normally) be about education and convincing the public (and the organization) that the protesters' cause is valid. Protesting, even in a digital reality, should not about forcing people. Convincing people takes communication, and DDoS is exactly the opposite; it is the denial of communication, and domination by force.

7 Bibliography

1. Make distributed denial-of-service (DDoS) a legal form of protesting. 2013 [cited 2013 11 Jan.]; Available from: https://petitions.whitehouse.gov/petition/make-distributed-denial-service-ddos-legal-form-protesting/X3drjwZY.
2. Bell, D., An introduction to cybercultures2001: Routledge.
3. Escobar, A., et al., Welcome to Cyberia: Notes on the Anthropology of Cyberculture [and comments and reply]. Current anthropology, 1994. 35(3): p. 211-231.
4. Assembly, U.N.G., Universal declaration of human rights. Resolution adopted by the General Assembly, 1948. 10(12).
5. Rao, L. Secretary Clinton: The Internet Has Become The World's Town Square. 2011 15 Feb. [cited 2013; Available from: http://techcrunch.com/2011/02/15/secretary-clinton-the-internet-has-become-the-worlds-town-square/.
6. Computer Fraud and Abuse Act, in 18 U.S.C. § 10301986: United States of America.
7. Taking part in industrial action and strikes. n.d. [cited 2013 15 Jan.]; Available from: https://http://www.gov.uk/industria action-strikes/going-on-strike-and-picketing.