Human Rights Protocol Considerations Research Group J. Varon
Internet-Draft Coding Rights
Intended status: Informational N. ten Oever
Expires: July 30, 2016 Article19
C. Guarnieri
Centre for Internet and Human Rights
W. Scott
University of Washington
C. Cath
Oxford Internet Institute
January 27, 2016

Human Rights Protocol Considerations Methodology
draft-varon-hrpc-methodology-03

Abstract

This document presents steps undertaken for developing a methodology to map engineering concepts at the protocol level that may be related to promotion and protection of Human Rights, particularly the right to freedom of expression and association. It aims to facilitate and build the work done by the Human Rights Protocol Considerations research group in the IRTF, as well as other authors within the IETF.

Exemplary work [RFC1984] [RFC6973] [RFC7258] has already been done in the IETF on privacy issues that should be considered when creating an Internet protocol. But, beyond privacy considerations, concerns for freedom of expression and association were also a strong part of the world-view of the community involved in developing the first Internet protocols. Indeed, promoting open, secure and reliable connectivity is essential for these rights. But how are this concepts addressed in the protocol level? Are there others? This ID is intended to explain research work done so far and to explore possible methodological approaches to move further on exploring and exposing the relations between standards and protocols and the promotion and protection of the rights to freedom of expression and association.

Discussion on this draft at: hrpc@irtf.org // https://www.irtf.org/mailman/listinfo/hrpc

working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 30, 2016.

Table of Contents

1. Introduction

In a manner similar to the work done for [RFC6973] on Privacy Consideration Guidelines, the premise of this research is that some standards and protocols can solidify, enable or threaten human rights.

As stated in [RFC1958], the Internet aims to be the global network of networks that provides unfettered connectivity to all users at all times and for any content. Our research hypothesis is that Internet's objective of connectivity makes it an enabler of human rights and that its architectural design tends to converge in protecting and promoting the human rights framework.

Open, secure and reliable connectivity is essential for human rights such as freedom of expression and freedom of association, as defined in the Universal Declaration of Human Rights [UDHR]. Therefore, considering connectivity as the ultimate objective of the Internet, makes a clear case that the Internet is not only an enabler of human rights, but that human rights lie at the basis of, and are ingrained in, the architecture of the network.

But, while the Internet was designed with freedom and openness of communications as core values, as the scale and the commercialization of the Internet has grown greatly, the influence of such world-views started to compete with other values. Therefore, decisive and human

rights enabling characteristics of the Internet might be degraded if they're not properly defined, described and protected as such. And, on the other way around, not protecting these characteristics could also result in (partial) loss of functionality and connectivity, thus, in the internet architecture design itself.

An essential part of maintaining the Internet as a tool for communication and connectivity is security. Indeed, "development of security mechanisms is seen as a key factor in the future growth of the Internet as a motor for international commerce and communication" [RFC1984] and according to the Danvers Doctrine [RFC3365], there is an overwhelming consensus in the IETF that the best security should be used and standardized.

In [RFC1984], the Internet Architecture Board (IAB) and the Internet Engineering Steering Group (IESG), the bodies which oversee architecture and standards for the Internet, expressed: "concern by the need for increased protection of international commercial transactions on the Internet, and by the need to offer all Internet users an adequate degree of privacy." Indeed, the IETF has been doing a significant job in this area [RFC6973] [RFC7258], considering privacy concerns as a subset of security concerns.

Besides privacy, it should be possible to highlight other aspects of connectivity embedded in standards and protocols that can have human rights considerations, such as freedom of expression and the right to association and assembly online. This ID is willing to explain research work done so far and explore possible methodological approaches to move further on exploring and exposing these relations between standards and protocols and the promotion and protection of the rights to freedom of expression and association.

To move this debate further, information has been compiled at the https://datatracker.ietf.org/rg/hrpc/ and discussions are happening through the list hrpc@irtf.org

This document builds on the previous IDs published within the framework of the hrpc research group [ID]

2. Research Topic

The growing impact of the Internet on the lives of individuals makes Internet standards and protocols increasingly important to society. The IETF itself, in [RFC2026], specifically states that the 'interests of the Internet community need to be protected'. There are various examples of protocols and standards having a direct impact on society, and by extension the human rights of end-users. Privacy is just one example. Therefore, this proposal for research

methodology is addressing as research topics the rights to freedom of expression and association and it's relations to standards and protocols.

These two rights are described in the Universal Declaration of Human Rights:

Article 19 - Freedom of Expression (FoE) "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."

Article 20 - Freedom of Association (FoA) "Everyone has the right to freedom of peaceful assembly and association."

But how to talk about human rights in an engineering context?

But can we translate these concepts into Internet architecture technical terms?

What standards and protocols could have any relationship with freedom of expression and association?

What are the possible relationships between them?

3. Methodology

Mapping the relation between human rights and protocols and architectures is a new research challenge, which requires a good amount of interdisciplinary and cross organizational cooperation to develop a consistent methodology. While the authors of this first draft are involved in both human rights advocacy and research on Internet technologies - we believe that bringing this work into the IRTF facilitates and improves this work by bringing human rights experts together with the community of researchers and developers of Internet standards and technologies.

In order to map the potential relation between human rights and protocols, so far, the HRPC research group has been gathering the data from three specific sources:

a. Discourse analysis of RFCs To start addressing the issue, a mapping exercise analyzing Internet architecture and protocols features, vis-a-vis possible impact on human rights is being undertaken. Therefore, research on the language used in current and historic RFCs and mailing list discussions is underway to expose core architectural principles, language and deliberations on human rights of those affected by the network.

b. Interviews with members of the IETF community during the Dallas meeting of March 2015 Interviews with the current and past members of the Internet Architecture Board (IAB), current and past members of the Internet Engineering Steering Group(IESG) and chairs of selected working groups and RFC authors. To get an insider understanding of how they view the relationship (if any) between human rights and protocols to play out in their work.

c. Participant observation in Working Groups By participating in various working groups information was gathered about the IETFs day-to-day work. From which which general themes and use-cases about human rights and protocols were extracted.

All this data was then processed using the following three consecutive strategies:

3.1. Translating Human Rights Concept into Technical Definitions

Step 1.1 - Mapping protocols and standards related to FoE and FoA Activity: Mapping of protocols and standards that potentially enable the internet as a tool for freedom of expression Expected Outcome: list of RFCs that describe standards and protocols that are potentially more closely related to FoE and FoA.

Step 1.2 - Extracting concepts from mapped RFCs Activity: Read the selected RFCs to highlight central design and technical concepts which impact human rights. Expected Outcome 1: a list of technical terms that combined create the enabling environment for freedom of expression and freedom of association. Expected Outcome 2: Possible translations of human rights concepts to technical terms.

Step 1.3 - Building a common glossary In the analysis of existing RFCs, central design and technical concepts shall be found which impact human rights. Expected Outcome: a Glossary for human rights protocol considerations with a list of concepts and definitions of technical concepts

3.2. Map cases of protocols being exploited or enablers

Step 1.1 - Cases of protocols being exploited Activity 1: Map cases in which users rights have been exploited, violated or compromised, analyze which protocols or vulnerabilities in protocols are invovled with this. Activity 2: Understand technical rationale for the use of particular protocols that undermine human rights. Expected Outcome: list of protocols that have been exploited to expose users to rights violation and rationale.

Step 1.2 - Cases of protocols being enablers Activity: Map cases in which users rights have been enabled, promoted and protected and analyze which characteristics in the protocols are involved with this. Expected Outcome: list of characteristics in the protocols that have been key to promote and protect the rights to freedom of expression and association that could be added to our glossary

3.3. Apply human rights technical definitions to the cases mapped

Step 1 - Glossary and Cases Activity: Investigate alternative technical options from within list of technical design principle (see [HRPC-GLOSSARY]) that could have been applied in the mapped cases to strengthen our technical definition of FoE and FoA, and hence human rights and connectivity of the network.

Expected Outcome: Identify best (and worst) current practices. Develop procedures to systematically evaluate protocols for potential human rights impact.

4. Preliminary findings achieved by applying current proposed methodology

4.1. Current status: Translating Human Rights Concept into Technical Definitions

Step 1.1 - Mapping protocols and standards related to FoE and FoA

Below are some examples of these protocols and standards that might be related to FoE and FoA and FoE:

HTTP Websites made it extremely easy for individuals to publish their ideas, opinions and thoughts. Never before has the world seen an infrastructure that made it this easy to share information and ideas with such a large group of other people. The HTTP architecture and standards, including [RFC7230], [RFC7231], [RFC7232], [RFC7234], [RFC7235], [RFC7236], and [RFC7237], are essential for the publishing of information. The HTTP protocol, therefore, forms an crucial enabler for freedom of expression, but also for the right to freely participate in the culture life of the community (Article 27) [UDHR], to enjoy the arts and to share in scientific advancement and its benefits.

Real time communications through XMPP and WebRTC Collaborations and cooperation via the Internet have take a large step forward with the progress of chat and other other real time communications protocols. The work on XMPP [RFC6162] has enabled new methods of global interactions, cooperation and human right advocacy. The WebRTC work being done to standardize the API and protocol elements to support

real-time communications for browsers, mobile applications and IoT by the World Wide Consortium (W3C) and the IETF is another artifact enabling human rights globally on the Internet.

Mailing lists Collaboration and cooperation have been part of the Internet since its early beginning, one of the instruments of facilitating working together in groups are mailing lists (as described in [RFC2639], [RFC2919], and [RFC6783]. Mailing lists are critical instruments and enablers for group communication and organization, and therefore form early artifacts of the (standardized) ability of Internet standards to enable the right to freedom of assembly and association.

IDNs English has been the lingua franca of the Internet, but for many Internet user English is not their first language. To have a true global Internet, one that serves the whole world, it would need to reflect the languages of these different communities. The Internationalized Domain Names IDNA2008 ([RFC5890], [RFC5891], [RFC5892], and [RFC5893]), describes standards for the use of a broad range of strings and characters (some also written from right to left). This enables users who use other characters than the standard LDH ascii typeset to have their own URLs. This shows the ambition of the Internet community to reflect the diversity of users and to be in line with Article 2 of the Universal Declaration of Human Rights which clearly stipulates that "everyone is entitles to all rights and freedoms "[...]", without distinction of any kind, such as "[...]" language "[...]"." [UDHR]

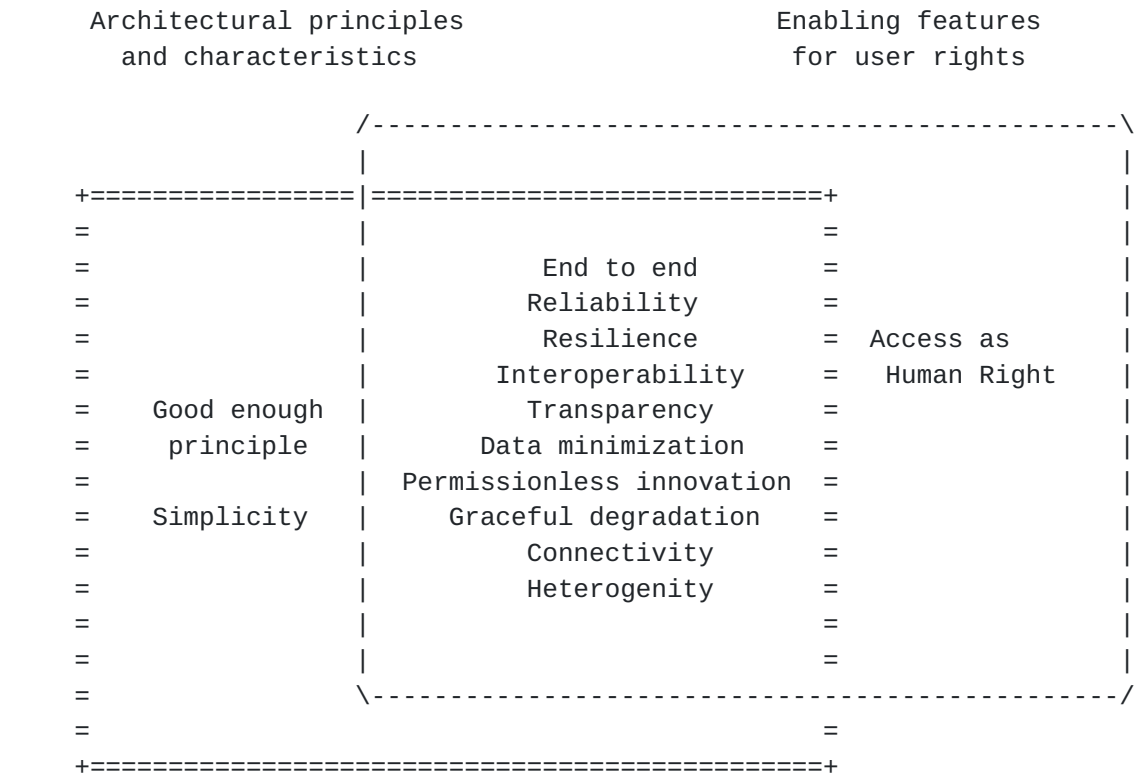
4.2. Current Status: Mapping protocols and standards related to FoE and FoA

Based on these standards and protocols as well as an analysis of existing RFCs and literature, a listing of architectural concepts has been made.

Step 1.2 - Extracting concepts from mapped RFCs The list of RFCs as well as relevant literature has used to extract key architectural principles. The main architectural concepts were subsequently listed in the glossary [HRPC-GLOSSARY].

4.3. Current Status: Extracting concepts from mapped RFCs

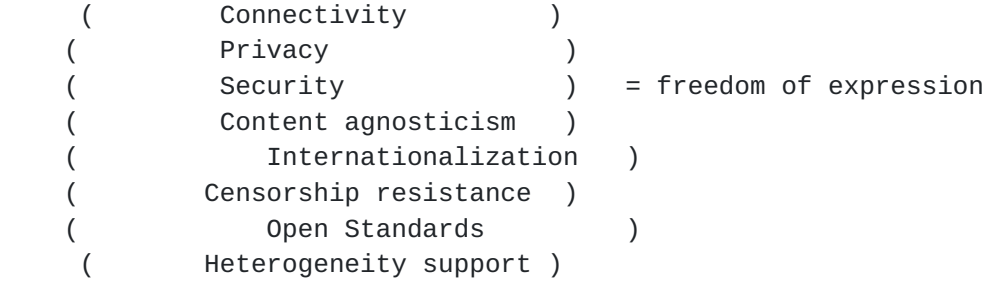
Expected Outcome 1: a list of technical terms that combined create the enabling environment for human rights, such a freedom of expression and freedom of association.

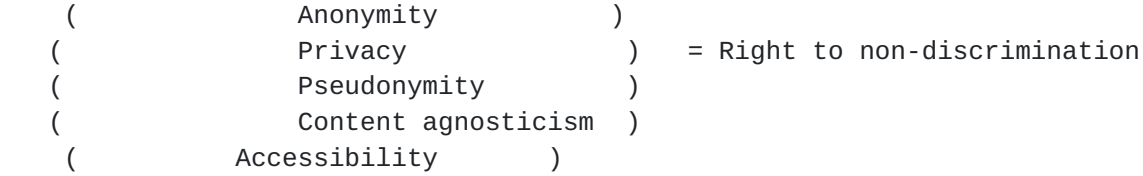


4.4. Current status: Translating human rights to technical terms

Expected outcome 2: This analysis aims to translate human rights concepts that impact or are impacted by the Internet as follows:

The combination of content agnosticism, connectivity, security, privacy (as defined in [RFC6973], and open standards are the technical principles that underlay freedom of expression on the Internet.





```
(            Content Agnosticism  )
(            Security             )    = Right to equal protection


 (           Anonymity       )
(            Privacy          )   = Right to be presumed innocent
 (           Security        )


 (      Accessibility         )
(       Internationalization   ) = Right to political participation
(       Censorship resistance  )
 (


 (  Open standards         )
(   Localization            ) = Right to participate in cultural life,
(   Internationalization    )             arts and science
 (  Censorship resistance  )


 (      Connectivity         )
(       Decentralization      )
(     Censorship resistance ) = Right to freedom of assembly
(       Pseudonymity          )                   and association
(       Anonymity             )
 (      Security             )


    ( Reliability    )
   (  Confidentiality )
   (  Integrity       ) = Right to security
   (  Authenticity    )
    ( Anonymity      )
```

Step 1.3 - Build a common glossary

4.5. Current status: Building of a common glossary

Expected Outcome: A glossary has been developed, which aims to build on other relevant published glossaries by the IETF and relevant literature: [HRPC-GLOSSARY]). This document aims to provide a description of relevant architectural principals as well as technical concepts that are relevant for describing the impact of protocols on human rights.

4.6. Current status: Map cases of protocols being exploited or enablers

4.6.1. IP

The Internet Protocol version 4, known as 'layer 3' of the internet, and specified as a common encapsulation and protocol header, is defined by [RFC0791]. The evolution of Internet communications have led to continued development in this area, encapsulated in the development of version 6 of the protocol in [RFC2460]. In spite of this updated protocol, we find that 25 years after the specification of version 6 of the protocol, the older v4 standard continues to account for a sizable majority of internet traffic.

The internet was designed as a platform for free and open communication, most notably encoded in the end-to-end principle, and that philosophy is also present in the technical implementation of the Internet Protocol. [RFC3724] While the protocol was designed to exist in an environment where intelligence is at the end hosts, it has proven to provide sufficient information that a more intelligent network core can make policy decisions and enforce policy shaping and restricting the communications of end hosts. These capabilities for network control and limitations of the freedom of expression by end hosts can be traced back to the IPv4 design, helping us understand which technical protocol decisions have led to harm of these human rights.

Two major shifts have occurred to harm freedom of expression through misuse of the Internet Protocol. The first is the network's exploitation of the public visibility of the host pairs for all communications, and the corresponding ability to discriminate and block traffic as a result of that metadata. The second is the selective development of IP options. Protocol extensions including Mobility and Multicasting have proposed alternate communication modes and suggest that different forms of assemply could be supported by an a robust IP layer. Instead, the protocol has limited the deployability of such extensions by not providing a mechanism for appropriate fallback behavior when unrecognized extensiosn are encountered.

4.6.1.1. Network visibility of Source and Destination

The IPv4 protocol header contains fixed location fields for both the source and destination IP addresses [RFC0791]. These addresses identify both the host sending and receiving each message, and allow the core network to understand who is talking to whom, and to practically limit communication selectively between pairs of hosts. Blocking of communication based on the pair of source and destination is one of the most common limitations on the ability for hosts to

communicate today, [caida] and can be seen as a restriction of the ability for those hosts to assemble or to consensually express themselves.

Inclusion of an Internet-wide identified source in the IP header is not the only possible design, especially since the protocol is most commonly implemented over Ethernet networks exposing only link-local identifiers. [RFC0894] A variety of alternative designs including source routing, and spoofing of the source IP address are technicaly supported by the protocol, but neither are regularly allowed on the Internet. While projects like [torproject] provide an alternative implementation of anonymity in connections, they have been developed in spite of the IPv4 protocol design.

4.6.1.2. Protocols

The other major feature of the IP protocol header is that it specifies the protocol encapsulated in each message in an easily observable form, and does not encourage a design where the encapsulated protocol is not available to a network observer. This design has resulted in a proliferation of routers which inspect the inner protocol, and has resulted in a stagnation where only the TCP and UDP protocols are widely supported across the Internet. While the IP protocol was designed as the entire set of metadata needed for routing, subsequent enhanced routers have found value on making policy decisions based on the contents of TCP and UDP headers as well, and are encoded with the assumption that only these protocols will be used for data transfer. [spdy] [RFC4303] defines an encrypted encapsulation of additional protocols, but lacks widespread deployment and faces the same challenge as any other protocol of providing sufficient metadata with each message for routers to make positive policy decisions. Protocols like [RFC4906] have seen limited wide-area uptake, and these alternate designs are frequently re-implemented on top of UDP. [quic]

4.6.1.3. Address Translation and Mobility

A major structural shift in the Internet which has undermined the protocol design of IPv4, and has significantly reduced the freedom of end users to communicate and assemble in the introduction network address translation. [RFC1631] Network address translation is a process whereby organizations and autonomous systems to connect two networks by translating the IPv4 source and destination addresses between the two. This process puts the router performing the translation into a privileged position, where it can decide which subset of communications are worthy of translation, and whether an unknown request for communication will be correctly forwarded to a host on the other network.

This process of translation has widespread adoption despite promoting a process that goes against the stated end-to-end process of the underlying protocol [natusage]. In contrast, the proposed mechanism to provide support for mobility and forwarding to clients which may move, encoded instead as an option in the IP protocol in [RFC5944], has failed to gain traction. This situation again suggests that the compromise made in design of the protocol has resulted in a technology which failed to technical encode the freedom of expression goals it was designed to promote.

4.6.2. DNS

The Domain Name System (DNS) [RFC1035], provides service discovery capabailities, and provides a mechanism to associate human readable names with services. The DNS system is organized around a set of independently operated 'Root Servers' run by organizations around the web which enact ICANN's policy by answering queries for which organizations have been delegated to manage registration under each Top Level Domain (TLD). Top Level domains are maintained and determined by ICANN. These namespaces encompass several classes of services. The initial name spaces including '.Com' and '.Net', provide common spaces for expression of ideas, though their policies are enacted through US based companies. Other name spaces are delegated to specific nationalities, and may impose limits designed to focus speech in those forums both to promote speech from that nationality, and to comply with local limits on expression and social norms. Finally, the system has been recently expanded with additional generic and sponsored name spaces, for instance '.travel' and '.ninja', which are operated by a range of organizations which may independently determine their registration policies.

DNS has significant privacy issues per [RFC7626]. Most notable are the lack of encryption to limit the visibility of requests for domain resolution from intermediary parties, and a limited deployment of DNSSEC to provide authentication, allowing the client to know that they have received a correct, "authoritative", answer to a query. Together, this situation results in ongoing harm to freedom of expression as interference with the operation of DNS has become one of the central mechanisms used to block access to websites. This interference limits both the freedom of expression of the publisher to offer their content, and the freedom of assembly for clients to congregate in a shared virtual space.

There have been several mechanisms used impose these limitations based on the technical design of the DNS protocol. These have led to a number of situations where limits on expression have been imposed through subversion of the DNS protocol. Each of these situations has accompanying aspects of protocol design enabling those limitations.

4.6.2.1. Removal of records

There have been a number of cases where the records for a domain are removed from the name system due to real-world events. Examples of this removal includes the 'seizure' of wikileaks [bbc-wikileaks] and the names of illegally operating gambling operations by the United States ICE unit, which compelled the US-based registry in charge of the .com TLD to hand ownership of those domains over to the government. The same technique has been notably used by Libya to remove sites in violation of "our Country's Law and Morality (which) do not allow any kind of pornography or its promotion." [techyum]

At a protocol level, there is no technical auditing for name ownership, as in alternate systems like [namecoin]. As a result, there is no ability for users to differentiate seizure from the legitimate transfer of name ownership, which is purely a policy decision of registrars. While DNSSEC addresses network distortion events described below, it does not tackle this problem, which has the cooperation of (or compelled action by) the registry.

4.6.2.2. Distortion of records

The most common mechanism by which the DNS system is abused to limit freedom of expression is through manipulation of protocol messages by the network. One form occurs at an organizational level, where client computers are instructed to use a local DNS resolver controlled by the organization. The DNS resolver will then selectively distort responses rather than request the authoritative lookup from the upstream system. The second form occurs through the use of deep packet inspection, where all DNS protocol messages are inspected by the network, and objectionable content is distorted, as in [turkey].

A notable instance of distortion has occurred in Greece [ververis], where a study found evidence of both of deep packet inspection to distort DNS replies, and overblocking of content, where ISPs prevented clients from resolving the names of domains which they were not instructed to do through the governmental order prompting the blocking systems there.

At a protocol level, the effectiveness of these attacks is made possible by a lack of authentication in the DNS protocol. DNSSEC provides the ability to determine authenticity of responses when used, but it is not regularly checked by resolvers. DNSSEC is not effective when the local resolver for a network is complicit in the distortion, for instance when the resolver assigned for use by an ISP is the source of injection. Selective distortion of records has also been made possible by the predictable structure of DNS messages,

which make it computationally easy for a network device to watch all passing messages even at high speeds, and the lack of encryption, which allows the network to distort only an objectionable subset of protocol messages. Specific distortion mechanisms are discussed further in [draft-hall-censorship-tech-01].

4.6.2.3. Injection of records

Responding incorrectly to requests for name lookups is the most common mechanism that in-network devices use to limit the ability of end users to discover services. A deviation which accomplishes a similar objective, though may be seen as different from a freedom of expression perspective, is the injection of incorrect responses to queries. The most prominent example of this behavior occurs in China, where requests for lookups of sites which have been deemed inappropriate will trigger the network to respond with a bogus response, causing the client to ignore the real response when it subsequently arrives. [greatfirewall] Unlike the other forms of discussion discussed above, injection does not stifle the ability of a server to announce it's name, it instead provides another voice which answers sooner. This is effective because without DNSSEC, the protocol will respond to whichever answer is received first, without listening for subsequent answers.

4.6.3. HTTP

The Hypertext Transfer Protocol (HTTP), described in its version 1.1 in RFC 7230 to 7237, is a request-response application protocol developed throughout the 1990s, and factually contributed to the exponential growth of the Internet and the inter-connection of populations around the world. Because of its simple design, HTTP has become the foundation of most modern Internet platforms and communication systems, from websites, to chat systems, and computer-to-computer applications. In its manifestation with the World Wide Web, HTTP has radically revolutionized the course of technological development and the ways people interact with online content and with each other. However, HTTP is also a fundamentally insecure protocol, that doesn't natively provide encryption properties. While the definition of the Secure Sockets Layer (SSL), and later of Transport Layer Security (TLS), also happened during the 1990s, the fact that HTTP doesn't mandate the use of such encryption layers to developers and service providers, caused a very late adoption. Only in the middle of the 2000s we observed big Internet service providers, such as Google, starting to provide encrypted access to their web services.

The lack of sensitivity and understanding of the critical importance of securing web traffic incentivized malicious and offensive actors

to develop, deploy and utilize at large interception systems and later active injection attacks, in order to swipe large amounts of data, compromise Internet-enabled devices. The commercial availability of systems and tools to perform these types of attacks also led to a number of human rights abuses that have been discovered and reported over the years and that painted a dark picture on the current state of control over the Internet.

Generally we can identify in Traffic Interception and Traffic Manipulation the two most problematic attacks that can be performed against applications employing a clear-text HTTP transport layer.

4.6.3.1. Traffic Interception

While we are seeing an increasing trend in the last couple of years to employ SSL/TLS as a secure traffic layer for HTTP-based applications, we are still far from seeing an ubiquitous use of encryption on the World Wide Web. It is important to consider that the adoption of SSL/TLS is also a relatively recent phenomena. Google introduced an option for its GMail users to navigate with SSL only in 2008 [Rideout], and turned SSL on by default later in 2010 [Schillace]. It took an increasing amount of scandalous security breaches and revelations on global surveillance from Edward Snowden to have other Internet service providers to follow Google's lead. For example, Yahoo enabled SSL/TLS by default on its webmail services only towards the end of 2013 [Peterson].

As we learned through the Snowden's revelations, intelligence agencies have been intercepting and collecting unencrypted traffic at large for many years. There are documented examples of such mass surveillance programs with GCHQ's TEMPORA and NSA's XKEYSCORE. Through these programs NSA/GCHQ have been able to swipe large amounts of data including email and instant messaging communications which have been transported by the respective providers in clear for years, unsuspecting of the pervasiveness and scale of governments' efforts and investment into global mass surveillance capabilities.

However, similar mass interception of unencrypted HTTP communications is also often employed at a nation-level by less democratic countries by exercising control over state-owned Internet Service Providers (ISP) and through the use of commercially available monitoring, collection, and censorship equipment. Over the last few years a lot of information has come to public attention on the role and scale of a surveillance industry dedicated to develop interception gear of different types. We have several records of such equipment being sold and utilized by oppressive regimes in order to monitor entire segments of population especially at times of social and political distress, uncovering massive human rights abuses. For example, in

2013 the group Telecomix revealed that the Syrian regime was making use of BlueCoat products in order to intercept clear-text traffic as well as to enforce censorship of unwanted content [RSF]. Similarly in 2012 it was found that the French Amesys provided the Gaddafi's government with equipment able to intercept emails, Facebook traffic, and chat messages ad a country level. The use of such systems, especially in the context of the Arab Spring and of civil uprisings against the dictatorships, has caused serious concerns of significant human rights abuses in Libya.

4.6.3.2. Traffic Manipulation

The lack of a secure transport layer over HTTP connections not only exposes the users to interception of the content of their communications, but is more and more commonly abused as a vehicle for active compromises of computers and mobile devices. If an HTTP session travels in clear over the network, any node positioned at any point in the network is able to perform man-in-the-middle attacks and observe, manipulate, and hijack the session and modify the content of the communication in order to trigger unexpected behavior by the application generating the traffic. For example, in the case of a browser the attacker would be able to inject malicious code in order to exploit vulnerabilities in the browser or any of its plugins. Similarly, the attacker would be able to intercept, trojanize, and repackage binary software updates that are very commonly downloaded in clear by applications such as word processors and media players. If the HTTP session would be encrypted, the tampering of the content would not be possible, and these network injection attacks would not be successful.

While traffic manipulation attacks have been long known, documented, and prototyped especially in the context of WiFi and LAN networks, in the last few years we observed an increasing investment into the production and sale of network injection equipment both available commercially as well as deployed at scale by intelligence agencies. For example we learned from some of the documents provided by Edward Snowden to the press, that the NSA has constructed a global network injection infrastructure, called QUANTUM, able to leverage mass surveillance in order to identify targets of interests and subsequently task man-on-the-side attacks to ultimately compromise a selected device. Among other attacks, NSA makes use of an attack called QUANTUMINSERT [Haagsma] which intercepts and hijacks an unencrypted HTTP communication and forces the requesting browser to redirect to a host controlled by NSA instead of the intended website. Normally, the new destination would be an exploitation service, referred in Snowden documents as FOXACID, which would attempt at executing malicious code in the context of the target's browser. The Guardian reported in 2013 that NSA has for example been using these

techniques to target users of the popular anonymity service Tor [Schneier]. The German NDR reported in 2014 that NSA has also been using its mass surveillance capabilities to identify Tor users at large [Appelbaum]. Recently similar capabilities of Chinese authorities have been reported as well in what has been informally called the "Great Cannon" [Marcak], which raised numerous concerns on the potential curb on human rights and freedom of speech due to the increasing tighter control of Chinese Internet communications and access to information. Network injection attacks are also made widely available to state actors around the world through the commercialization of similar, smaller scale equipment that can be easily acquired and deployed at a country-wide level. Companies like FinFisher and HackingTeam are known to have network injection gear within their products portfolio, respectively called FinFly ISP and RCS Network Injector [Marquis-Boire]. The technology devised and produced by HackingTeam to perform network traffic manipulation attacks on HTTP communications is even the subject of a patent application in the United States [Googlepatent]. Access to offensive technologies available on the commercial lawful interception market has been largely documented to have lead to human rights abuses and illegitimate surveillance of journalists, human rights defenders, and political activists in many countries around the world. Companies like FinFisher and HackingTeam have been found selling their products to oppressive regimes with little concern for bad human rights records [Collins]. While network injection attacks haven't been the subject of much attention, they do enable even unskilled attackers to perform silent and very resilient compromises, and unencrypted HTTP remains one of the main vehicles.

4.6.4. XMPP

The Extensible Messaging and Presence Protocol (XMPP), specified in RFC 6120, provides a standard for interactive chat messaging, and has evolved to encompass interoperable text, voice, and video chat. The protocol is structured as a federated network of servers, similar to email, where users register with a local server which acts one their behalf to cache and relay messages. This protocol design has many advantages, allowing servers to shield clients from denial of service and other forms of retribution for their expression, and designed to avoid central entities which could control the ability to communicate or assemble using the protocol.

None-the-less, there are plenty of aspects of the protocol design of XMPP which shape the ability for users to communicate freely, and to assembly through the protocol. The protocol also has facets that may stifle speech as users self-censor for fear of surveillance, or find themselves unable to express themselves naturally.

4.6.4.1. User Identification

The XMPP specification dictates that clients are identified with a resource (node@domain/home [1] / node@domain/work [2]) to distinguish the conversations to specific devices. While the protocol does not specify that the resource must be exposed by the client's server to remote users, in practice this has become the default behavior. In doing so, users can be tracked by remote friends and their servers, who are able to monitor presence not just of the user, but of each individual device the user logs in with. This has proven to be misleading to many users, [pidgin] since many clients only expose user level rather than device level presence. Likewise, user invisibility so that communication can occur while users don't notify all buddies and other servers of their availability is not part of the formal protocol, and has only been added as an extension within the XML stream rather than enforced by the protocol.

4.6.4.2. Surveillance of Communication

The XMPP protocol specifies the standard by which communication of channels may be encrypted, but it does not provide visibility to clients of whether their communications are encrypted on each link. In particular, even when both clients ensure that they have an encrypted connection to their XMPP server to ensure that their local network is unable to read or disrupt the messages they send, the protocol does not provide visibility into the encryption status between the two servers. As such, clients may be subject to selective disruption of communications by an intermediate network which disrupts communications based on keywords found through Deep Packet Inspection. While many operators have commited to only establishing encrypted links from their servers in recognition of this vulnerability, it remains impossible for users to audit this behavior and encrypted connections are not required by the protocol itself [xmppmanifesto].

In particular, section 13.14 of the protocol specification [RFC6120] explicitly acknowledges the existence of a downgrade attack where an adversary controlling an intermediate network can force the inter domain federation between servers to revert to a non-encrypted protocol were selective messages can then be disrupted.

4.6.4.3. Group Chat Limitations

Group chat in the XMPP protocol is defined as an extension within the XML specification of the XMPP protocol (https://xmpp.org/extensions/xep-0045.html). However, it is not encoded or required at a protocol level, and not uniformly implemented by clients.

The design of multi-user chat in the XMPP protocol suffers from extending a protocol that was not designed with assembly of many users in mind. In particular, in the federated protocol provided by XMPP, multi-user communities are implemented with a distinguished 'owner', who is granted control over the participants and structure of the conversation.

Multi-user chat rooms are identified by a name specified on a specific server, so that while the overall protocol may be federated, the ability for users to assemble in a given community is moderated by a single server. That server may block the room and prevent assembly unilaterally, even between two users neither of whom trust or use that server directly.

4.6.5. Peer to Peer

Peer-to-Peer (P2P) is a network architecture (defined in RFC7574) in which all the participant nodes are equally responsible engaged into the storage and dissemination of information. A P2P network is a logical overlay that lives on top of the physical network, and allows nodes (or "peers") participating to it to establish contact and exchange information directly from one to each other. The implementation of a P2P network may very widely: it may be structured or unstructured, and it may implement stronger or weaker cryptographic and anonymity properties. While its most common application has traditionally been file-sharing (and other types of content delivery systems), P2P is increasingly becoming a popular architecture for networks and applications that require (or encourage) decentralization. A prime example is Bitcoin (and similar cryptocurrencies), as well as Skype, Spotify and other proprietary multimedia applications.

In a time of heavily centralized online services, peer-to-peer is often seen as an alternative, more democratic, and resistant architecture that displaces structures of control over data and communications and delegates all peers equally to be responsible for the functioning, integrity, and security of the data. While in principle peer-to-peer remains critical to the design and development of future content distribution, messaging, and publishing systems, it poses numerous security and privacy challenges which are mostly delegated to individual developers to recognize, analyze, and solve in each implementation of a given P2P network.

4.6.5.1. Network Poisoning

Since content, and in some occasions peer lists, are safeguarded and distributed by its members, P2P networks are prone to what are generally defined as "poisoning attacks". Poisoning attacks might be

directed directly at the data that is being distributed, for example by intentionally corrupting it, or at the index tables used to instruct the peers where to fetch the data, or at routing tables, with the attempt of providing connecting peers with lists of rogue or non-existing peers, with the intention to effectively cause a Denial of Service on the network.

4.6.5.2. Throttling

Peer-to-Peer traffic (and BitTorrent in particular) represents a high percentage of global Internet traffic and it has become increasingly popular for Internet Service Providers to perform throttling of customers lines in order to limit bandwidth usage [torrentfreak1] and sometimes probably as an effect of the ongoing conflict between copyright holders and file-sharing communities [wikileaks].

Throttling the peer-to-peer traffic makes some uses of P2P networks ineffective and it might be coupled with stricter inspection of users' Internet traffic through Deep Packet Inspection techniques which might pose additional security and privacy risks.

4.6.5.3. Tracking and Identification

One of the fundamental and most problematic issues with traditional peer-to-peer networks is a complete lack of anonymization of its users. For example, in the case of BitTorrent, all peers' IP addresses are openly available to the other peers. This has lead to an ever-increasing tracking of peer-to-peer and file-sharing users [ars]. As the geographical location of the user is directly exposed, and so could be his identity, the user might become target of additional harassment and attacks, being of physical or legal nature. For example, it is known that in Germany lawfirms have made extensive use of peer-to-peer and file-sharing tracking systems in order to identify downloaders and initiate legal actions looking for compensations [torrentfreak2].

It is worth nothing that there are varieties of P2P networks that implement cryptographic practices and that introduce anonymization of its users. Such implementations proved to be successful in resisting censorship of content, and tracking of the network peers. A primary example is FreeNet [freenet1], a free software application designed to significantly increase the difficulty of users and content identification, and dedicated to foster freedom of speech online [freenet2].

4.6.5.4. Sybil Attacks

In open-membership P2P networks, a single attacker can pretend to be many participants, typically by creating multiple fake identities of whatever kind the P2P network uses [Douceur]. Attackers can use Sybil attacks to bias choices the P2P network makes collectively toward the attacker's advantage, e.g., by making it more likely that a particular data item (or some threshold of the replicas or shares of a data item) are assigned to attacker-controlled participants. If the P2P network implements any voting, moderation, or peer review-like functionality, Sybil attacks may be used to "stuff the ballots" toward the attacker's benefit. Companies and governments can use Sybil attacks on discussion-oriented P2P systems for "astroturfing" or creating the appearance of mass grassroots support for some position where there is none in reality.

4.6.5.5. Conclusions

Encrypted P2P and Anonymous P2P networks already emerged and provided viable platforms for sharing material, publish content anonymously, and communicate securely [bitmessage]. If adopted at large, well-designed and resistant P2P networks might represent a critical component of a futuresecure and distributed Internet, enabling freedom of speech and freedom of information at scale.

4.6.6. Virtual Private Network

4.6.6.1. Introduction

A Virtual Private Network (VPN) is a point-to-point connection that enables two computers to communicate over an encrypted tunnel. There are multiple implementations and protocols used in provisioning a VPN, and they generally diversify by encryption protocol or particular requirements, most commonly in proprietary and enterprise solutions. VPNs are used commonly either to enable some devices to communicate through peculiar network configurations, or in order to use some privacy and security properties in order to protect the traffic generated by the end user; or both. VPNs have also become a very popular technology among human rights defenders, dissidents, and journalists worldwide to avoid local illegitimate wiretapping and eventually also to circumvent censorship. Among human rights defenders VPNs are often debated as a potential alternative to Tor or other anonymous networks. Such comparison is mislead, as some of the privacy and security properties of VPNs are often misunderstood by less tech-savvy users, which could ultimately lead to unintended problems.

As VPNs increased in popularity, commercial VPN providers have started growing in business and are very commonly picked by human rights defenders and people at risk, as they are normally provided with an easy-to-use service and sometimes even custom applications to establish the VPN tunnel. Not being able to control the configuration of the network, and even less so the security of the application, assessing the general privacy and security state of common VPNs is very hard. Often such services have been discovered leaking information, and their custom applications have been found flawed. While Tor and similar networks receive a lot of scrutiny from the public and the academic community, commercial or non-commercial VPN networks are way less analyzed and understood, and it might be valuable to establish some standards to guarantee a minimal level of privacy and security to those who need them the most.

4.6.6.2. False sense of Anonymity

One of the common misconception among users of VPNs is the level of anonymity VPN can provide. This sense of anonymity can be betrayed by a number of attacks or misconfugrations of the VPN provider. It is important to remember that, contrarily to Tor and similar systems, VPN was not designed to provide anonymity properties. From a technical point of view, the VPN might leak identifiable information, or might be subject of correlation attacks that could expose the originating address of the connecting user. Most importantly, it is vital to understand that commercial and non-commercial VPN providers are bound by the law of the jurisdiction they reside in or in which their infrastructure is located, and they might be legally forced to turn over data of specific users if legal investigations or intelligence requirements dictate so. In such cases, if the VPN providers retain logs, it is possible that the information of the user is provided to the user's adversary and leads to his or her identification.

4.6.6.3. Logging

With VPN being point-to-point connections, the service providers are in fact able to observe the original location of the connecting users and they are able to track at what time they started their session and eventually also to which destinations they're trying to connect to. If the VPN providers retain logs for long enough, they might be forced to turn over the relevant data or they might be otherwise compromised, leading to the same data getting exposed. A clear log retaining policy could be enforced, but considering that countries enforce very different levels of data retention policies, VPN providers should at least be transparent on what information do they store and for how long is being kept.

4.6.6.4. 3rd Party Hosting

VPN providers very commonly rely on 3rd parties to provision the infrastructure that is later going to be used to run VPN endpoints. For example, they might rely on external dedicated server hosting providers, or on uplink providers. In those cases, even if the VPN provider itself isn't retaining any significant logs, the information on the connecting users might be retained by those 3rd parties instead, introducing an additional collection point for the adversary.

4.6.6.5. IPv6 Leakage

Some studies proved that several commercial VPN providers and applications suffer of critical leakage of information through IPv6 due to improper support and configuration [PETS2015VPN]. This is generally caused by a lack of proper configuration of the client's IPv6 routing tables. Considering that most popular browsers and similar applications have been supporting IPv6 by default, if the host is provided with a functional IPv6 configuration, the traffic that is generated might be leaked if the VPN application isn't designed to manipulate such traffic properly.

4.6.6.6. DNS Leakage

Similarly, VPN services that aren't handling DNS requests and are not running DNS servers of their own, might be prone to DNS leaking which might not only expose sensitive information on the activity of the user, but could also potentially lead to DNS hijacking attacks and following compromises.

4.6.6.7. Traffic Correlation

As revelations of mass surveillance have been growing in the press, additional details on attacks on secure Internet communications have come to the public's attention. Among these, VPN appeared to be a very interesting target for attacks and collectiong efforts. Some implementations of VPN appear to be particularly vulnerable to identification and collection of key exchanges which, some Snowden documents revealed, are systematically collected and stored for future reference. The ability of an adversary to monitor network connections at many different points over the Internet, can allow them to perform traffic correlation attacks and identify the origin of certain VPN traffic by cross referencing the connection time of the user to the endpoint and the connection time of the endpoint to the final destination. These types of attacks, although very expensive and normally only performed by very resourceful adversaries, have been documented [spiegel] to be already in practice

and could completely vanify the use of a VPN and ultimately expose the activity and the identity of a user at risk.

4.6.7. HTTP Status Code 451

Every Internet user has run into the '404 Not Found' Hypertext Transfer Protocol (HTTP) status code when trying, and failing, to access a particular website. It is a response status that the server sends to the browser, when the server cannot locate the URL. '403 Forbidden' is another example of this class of code signals that gives users information about what is going on. In the '403' case the server can be reached, but is blocking the request because the user is trying to access content forbidden to them. This can be because the specific user is not allowed access to the content (like a government employee trying to access pornography on a work-computer) or because access is restricted to all users (like social network sites in certain countries). As surveillance and censorship of the Internet is becoming more commonplace, voices were raised at the IETF to introduce a new status code that indicates when something is not available for 'legal reasons' (like censorship):

The 451 status code would allow server operators to operate with greater transparency in circumstances where issues of law or public policy affect their operation. This transparency may be beneficial both to these operators and to end-users [Bray].

The status code would be named '451', a reference to Bradbury's famous novel on censorship

During the IETF meeting in Dallas, there was discussion about the usefulness of '451'. The main tension revolved around the lack of an apparent machine-readable technical use of the information. The extent to which '451' is just 'political theatre' or whether it has a concrete technical use was heatedly debated. Some argued that 'the 451 status code is just a status code with a response body' others said it was problematic because 'it brings law into the picture'. Again others argued that it would be useful for individuals, or organizations like the 'Chilling Effects' project, crawling the web to get an indication of censorship (IETF discussion on '451' - author's field notes March 2015). There was no outright objection during the Dallas meeting against moving forward on status code '451', and on December 18, 2015 the Internet Engineering Steering Group approved publication of 'An HTTP Status Code to Report Legal Obstacles'. It is still in the process of becoming an RFC, but could effectively be used from the day of approval.

What is interesting about this particular case is that not only technical arguments but also the status code's outright potential

political use for civil society played a substantial role in shaping the discussion, and the decision to move forward with this technology.

It is however important to note that 451 is not a solution to detect all occasions of censorship. A large swath of Internet filtering occurs in the network rather than the server itself. For these forms of censorship 451 plays a limited role, as the servers will not be able to send the code, because they haven't received the requests (as is the case with servers with resources blocked by the Chinese Golden shield). Such filtering regimes are unlikely to voluntarily inject a 451 status code. The use of 451 is most likely to apply in the case of cooperative, legal versions of content removal resulting from requests to providers. One can think of content that is removed or blocked for legal reasons, like copyright infringement, gambling laws, child abuse, et cetera. The major use case is thus clearly on the Web server itself, not the network. Large Internet companies and search engines are constantly asked to censor content in various jurisdictions. 451 allows this to be easily discovered, for instance by initiatives like the Lumen Database. In the case of adversarial blocking done by a filtering entity on the network 451 is less useful.

Overall, the strength of 451 lies in its ability to provide transparency by giving the reason for blocking, and giving the end-user the ability to file a complaint. It allows organizations to easily measure censorship in an automated way, and prompts the user to access the content via another path (e.g. TOR, VPNs) when (s)he encounters the 451 status code.

Status code 451 impact human rights by making censorship more transparent and measurable. THe status code increases transparency both by signaling the existence of censorship (instead of a much more broad HTTP error message like HTTP status code 404) as well as providing details of the legal restriction, which legal authority is imposing it, and what class of resources it applies to. This empowers the user to seek redress.

4.6.8. Middleboxes

On the current Internet, transparency on how packets reach a destination is no longer a given. This is due to the increased presence of firewalls, spam filters, and network address translators networks (NATs) - or middleboxes as these hosts are often called - that make use of higher-layer fields to function [Walfish]. This development is contentious. The debate also unfolded at the IETF, specifically at the Session Protocol Underneath Datagrams (SPUD) Birds of a Feather (BOF) meeting held at the IETF conference in March

2015. The discussion at the BOF focused on questions about adding meta-data, or other information to traffic flows, to enable the sharing of information with middleboxes in that flow. During the sessions two competing arguments were distilled. On the one hand adding additional data would allow for network optimization, and hence improve traffic carriage. On the other hand, there are risks of information leakage and other privacy and security concerns. Middleboxes, and the protocols guiding them, influence individuals' ability to communicate online freely and privately. Repeatedly mentioned in the discussion was the danger of censorship that comes with middleboxes, and the IETF's role to prevent such censorship from happening. Middleboxes are becoming a proxy for the debate on the extent to which commercial interests are a valid reason to undermine the end-to-end principle. The potential for abuse and censoring, and thus ultimately the impact of middleboxes on the Internet as a place of unfiltered, unmonitored freedom of speech, is real. It is impossible to make any definitive statements about the direction the debate on middleboxes will take at the IETF. The opinions expressed in the SPUD BOF and by the various interviewees indicate that a majority of engineers are trying to mitigate the negative effects of middleboxes on freedom of speech, but their ability to act is limited by their larger commercial context that is expanding the use of middleboxes.

4.6.9. DDOS attacks

Are Distributed Denial of Service (DDoS) attacks a legitimate form of online protest protected by the right to freedom of speech and association? Can they be seen as the equivalent to 'million-(wo)men marches', or sit-ins? Or are they a threat to freedom of expression and access to information, by limiting access to websites and in certain cases the freedom of speech of others? These questions are crucial in our day and age, where political debates, civil disobedience and other forms of activism are increasingly moving online.

Many individuals, not excluding IETF engineers, have argued that DDoS attacks are fundamentally against freedom of speech. Technically DDoS attacks are when multiple computers overload the bandwidth or resources of a website (or other system) by flooding it with traffic, causing it to temporarily stop being available to users. In their 2010 report Zuckerman et al argue that DDoS attacks are a bad thing because they are increasingly used by governments to attack and silence critics. Their research demonstrates that in many countries independent media outlets and human rights organizations are the victim of DDoS attacks, which are directly or indirectly linked to their governments. These types of attacks are particularly complicated because attribution is difficult, creating a situation in

which governments can effectively censor content, while being able to deny involvement in the attacks [Zuckerman]. DDoS attacks can thus stifle freedom of expression, complicate the ability of independent media and human rights organizations to exercise their right to (online) freedom of association, while facilitating the ability of governments to censor dissent. When it comes to comparing DDoS attacks to protests in offline life, it is important to remember that only a limited number of DDoS attacks involved solely willing participants. In most cases, the clients are hacked computers of unrelated parties that have not consented to being part of a DDoS (for exceptions see Operation Abibil [Abibil] or the Iranian Green Movement DDoS [GreenMovement]).

In addition, DDoS attacks are increasingly used as an extortion tactic, with criminals flooding a website - rendering it inaccessible - until the owner pays them a certain amount of money to stop the attack. The costs of mitigating such attacks, either by improving security to prevent them or paying off the attackers, ends up being paid by the consumer.

All of these issues seem to suggest that the IETF should try to ensure that their protocols cannot be used for DDoS attacks. Decreasing the number of vulnerabilities in the network stacks of routers or computers, reducing flaws in HTTPS implementations, and depreciating non-secure HTTP protocols could address this issue. The IETF can clearly play a role in bringing about some of these changes, and has indicated in RFC 7258 its commitment to mitigating 'pervasive monitoring (...) in the design of IETF protocols, where possible.' This means the use of encryption should become standard. Effectively, for the web this means standardized use of HTTPS. The IETF could redirect its work such that HTPPS becomes part-and-parcel of its standards. However, next to the various technical trade-offs that this might lead to it is important to consider that DDoS attacks are sometimes seen as a method for exercising freedom of speech.

DDoS although disruptive, and silencing at times, can also enable as protest and speech. Or as Sauter [Sauter] argues: 'though DDoS as a tactic is still relatively novel, it fits within a centuries- long tradition of breaking laws and disrupting business as usual to make a political point. These actions aren't simply disruption for disruption's sake. Rather they serve to help the activist or dissenter to direct the attention of the public through the interpolation of difference into routine.' (30-31). An often heard argument against DDoS attacks is that you cannot construe it as a means to exercise your right to freedom of speech, when the means used effectively impede the right of the party on the receiving end of the attack to exercise that same right. The problem with this line of argumentation is that it conveniently ignores the fact that

online DDoS attacks are often one of the few effective ways for activists to gain the attention of the media, the government or other parties of interest. Simply putting up a website for a cause won't garner the same amount of attention as directly confronting the issue via the website of the individual or organization at the heart of the issue. The ability of activists to do so should be protected, especially considering the fact that as Sauter (2014:4) explains: 'Collectively, we have allowed the construction of an entire public sphere, the Internet, which by accidents of evolution and design, has none of the inherent free speech guarantees we have come to expect. Dissenting voices are pushed out of the paths of potential audiences, effectively removing them from the public discourse. There is nowhere online for an activist to stand with her friends and her sign. She might set up a dedicated blog--which may or may not ever be read--but it is much harder for her to stand collectively with others against a corporate giant in the online space.' Although the Internet is often compared to public space, it is not. Rather the opposite. The Internet is almost entirely owned by private entities. And the IETF plays a crucial role in developing this privatized commercialized Internet.

From a legal and political perspective, the IETF does not have the legitimacy to determine when a DDoS is legitimate (in legal or political terms). It does not have the capability to make this judgment as a matter of public policy and subsequently translate it to code. Nor should the IETF try to do so. From a technical perspective, the difference between a 'legitimate' and 'illegitimate' DDoS attack is meaningless because it would be extremely difficult for the IETF to engineer a way to detect that difference. In addition, there is a need for the IETF to be consistent in the face of attacks (an attack is an attack is an attack) to maintain the viability of the network. Arguing that some DDoS attacks should be allowed, based on the motivation of the attackers complicates the work of the IETF. Because it approaches PM regardless of the motivation of the attackers (see RFC 7258 for why), taking the motivation of the attackers into account for DDoS would indirectly undermine the ability of the IETF to protect the right to privacy because it introduces an element of inconsistency into how the IETF deals with attacks.

David Clark recently published a paper warning that the future of the Internet is in danger. He argues that the private sector control over the Internet is too strong, limiting the myriad of ways in which it can be used [Daedalus], including for freedom of speech. But just because freedom of speech, dissent, and protest are human rights, and DDoS is a potential expression of those rights, doesn't mean that DDoS in and of itself is a right. To widen the analogy, just because the Internet is a medium through which the right to freedom of

expression can be exercised does not make access to the Internet or specific ICTs or NCTs a human right. Uses of DDoS might or might not be legitimate for political reasons, but the IETF has no means or methods to assess this, and in general enabling DDoS would mean a deterioration of the network and thus freedom of expression.

In summation, the IETF cannot be expected to take a moral stance on DDoS attacks, or create protocols to enable some attacks and inhibit others. But what it can do is critically reflect on its role in creating a commercialized Internet without a defacto public space or inherent protections for freedom of speech.

5. Next Steps of the Methodology still to be applied

5.1. Apply human rights technical definitions to the cases mapped

6. Next Steps of the Methodology still to be developed

6.1. Future research questions

All of the steps mentioned above raise the following question that need to be addressed after the research methodological steps outlined above have been completed:

How can the rights enabling environment be safeguarded in (future) protocol development?

How can (nontransparent) human rights violations be minimized in (future) protocol development?

Can we propose guidelines to protect the Internet as a human-rights-enabling environment in future protocol development, specially in relation to freedom of expression and freedom of association, in a manner similar to the work done for Privacy Considerations in [RFC6973]?

Assuming that the research produces useful results, can the objective evolve into the creation of a set of recommended considerations for the protection of applicable human rights?

7. Acknowledgements

Special thanks to all members of the hrpc RG who contributed to this draft. The following deserve a special mention: Stephane Bortzmeyer, dkg and Tim Sammut.

8. Security Considerations

As this draft concerns a research document, there are no security considerations.

9. IANA Considerations

This document has no actions for IANA.

10. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations proposed working group is located at the e-mail address hrpc@ietf.org [3]. Information on the group and information on how to subscribe to the list is at https://www.irtf.org/mailman/listinfo/hrpc

Archives of the list can be found at: https://www.irtf.org/mail-archive/web/hrpc/current/index.html

11. References

11.1. Informative References

[Abibil] Danchev, D., "Dissecting 'Operation Ababil' - an OSINT Analysis", 2012, <http://ddanchev.blogspot.be/2012/09/dissecting-operation-ababil-osint.html>.

[Appelbaum] Appelbaum, J., Gibson, A., Kabish, V., Kampf, L., and L. Ryge, "NSA targets the privacy-conscious", 2015, <http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html>.

[ars] Anderson, N., "P2P researchers - use a blocklist or you will be tracked... 100% of the time", 2007, <http://arstechnica.com/uncategorized/2007/10/p2p-researchers-use-a-blocklist-or-you-will-be-tracked-100-of-the-time/>.

[bbc-wikileaks] BBC, "Whistle-blower site taken offline", 2008, <http://news.bbc.co.uk/2/hi/technology/7250916.stm>.

[bitmessage] Bitmessage, "Bitmessage Wiki?", 2014, <https://bitmessage.org/wiki/Main_Page>.

[Bray] Bray, T., "A New HTTP Status Code for Legally-restricted Resources", 2016, <https://tools.ietf.org/html/draft-ietf-httpbis-legally-restricted-status-04>.

[caida] Dainotti, A., Squarcella, C., Aben, E., Claffy, K., Chiesa, M., Russo, M., and A. Pescape, "Analysis of Country-wide Internet Outages Caused by Censorship", 2013, <http://www.caida.org/publications/papers/2014/outages_censorship/outages_censorship.pdf>.

[Collins] Collins, K., "Hacking Team's oppressive regimes customer list revealed in hack", 2015, <http://www.wired.co.uk/news/archive/2015-07/06/hacking-team-spyware-company-hacked>.

[Daedalus] Clark, D., "The Contingent Internet", Daedalus Winter 2016, Vol. 145, No. 1. p. 9-17 , 2016, <http://www.mitpressjournals.org/toc/daed/current>.

[Douceur] Douceur, J., "The Sybil Attack", 2002, <http://research.microsoft.com:8082/pubs/74220/IPTPS2002.pdf>.

[draft-hall-censorship-tech-01] Hall, J., Aaron, M., and B. Jones, "A Survey of Worldwide Censorship Techniques", 2015, <https://tools.ietf.org/html/draft-hall-censorship-tech-01>.

[freenet1] Freenet, "What is Freenet?", n.d., <https://freenetproject.org/whatis.html>.

[freenet2] Ian Clarke, ., "The Philosphy behind Freenet?", n.d., <https://freenetproject.org/philosophy.html>.

[Googlepatent] Google, ., "Method and device for network traffic manipulation", 2012, <https://www.google.com/patents/EP2601774A1?cl=en>.

[greatfirewall] Anonymous, ., "Towards a Comprehensive Picture of the Great Firewall's DNS Censorship", 2014, <https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf>.

[GreenMovement]
Villeneuve, N., "Iran DDoS", 2009, <https://www.nartv.org/2009/06/16/iran-ddos/>.

[Haagsma] Haagsma, L., "Deep dive into QUANTUM INSERT", 2015, <http://blog.fox-it.com/2015/04/20/deep-dive-into-quantum-insert/>.

[HRPC-GLOSSARY]
ten Oever, N., Doria, A., and D. Gillmor, "Human Rights Protocol Considerations Glossary", 2015, <https://www.ietf.org/id/draft-dkg-hrpc-glossary-00.txt>.

[ID] ten Oever, N., Doria, A., and J. Varon, "Proposal for research on human rights protocol considerations", 2015, <http://tools.ietf.org/html/draft-doria-hrpc-proposal>.

[Marcak] Marcak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott-Railton, J., Deibert, R., and V. Paxson, "China's Great Fire Cannon", 2015, <https://citizenlab.org/2015/04/chinas-great-cannon/>.

[Marquis-Boire]
Marquis-Boire, M., "Schrodinger's Cat Video and the Death of Clear-Text", 2014, <https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text/>.

[namecoin]
Namecoin, "Namecoin - Decentralized secure names", 2015, <https://namecoin.info/>.

[natusage]
Maier, G., Schneider, F., and A. Feldmann, "NAT usage in Residential Broadband networks", 2011, <http://www.icsi.berkeley.edu/pubs/networking/NATusage11.pdf>.

[Peterson]
Peterson, A., Gellman, B., and A. Soltani, "Yahoo to make SSL encryption the default for Webmail users. Finally.", 2013, <http://gmailblog.blogspot.de/2010/01/default-https-access-for-gmail.html>.

[PETS2015VPN]
Pera, V., Barbera, M., Tyson, G., Haddadi, H., and A. Mei, "A Glance through the VPN Looking Glass", 2015, <http://www.eecs.qmul.ac.uk/~hamed/papers/PETS2015VPN.pdf>.

[pidgin] js, . and Pidgin Developers, "-XMPP- Invisible mode violating standard", July 2015, <https://developer.pidgin.im/ticket/4322>.

[quic] The Chromium Project, "QUIC, a multiplexed stream transport over UDP", 2014, <https://www.chromium.org/quic>.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <http://www.rfc-editor.org/info/rfc791>.

[RFC0894] Hornig, C., "A Standard for the Transmission of IP Datagrams over Ethernet Networks", STD 41, RFC 894, DOI 10.17487/RFC0894, April 1984, <http://www.rfc-editor.org/info/rfc894>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <http://www.rfc-editor.org/info/rfc1035>.

[RFC1631] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, DOI 10.17487/RFC1631, May 1994, <http://www.rfc-editor.org/info/rfc1631>.

[RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996, <http://www.rfc-editor.org/info/rfc1958>.

[RFC1984] IAB and , "IAB and IESG Statement on Cryptographic Technology and the Internet", BCP 200, RFC 1984, DOI 10.17487/RFC1984, August 1996, <http://www.rfc-editor.org/info/rfc1984>.

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, <http://www.rfc-editor.org/info/rfc2026>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC2639] Hastings, T. and C. Manros, "Internet Printing Protocol/1.0: Implementer's Guide", RFC 2639, DOI 10.17487/RFC2639, July 1999, <http://www.rfc-editor.org/info/rfc2639>.

[RFC2919] Chandhok, R. and G. Wenger, "List-Id: A Structured Field and Namespace for the Identification of Mailing Lists", RFC 2919, DOI 10.17487/RFC2919, March 2001, <http://www.rfc-editor.org/info/rfc2919>.

[RFC3365] Schiller, J., "Strong Security Requirements for Internet Engineering Task Force Standard Protocols", BCP 61, RFC 3365, DOI 10.17487/RFC3365, August 2002, <http://www.rfc-editor.org/info/rfc3365>.

[RFC3724] Kempf, J., Austein., R., Ed., and IAB, "The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture", RFC 3724, DOI 10.17487/RFC3724, March 2004, <http://www.rfc-editor.org/info/rfc3724>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <http://www.rfc-editor.org/info/rfc4303>.

[RFC4906] Martini, L., Ed., Rosen, E., Ed., and N. El-Aawar, Ed., "Transport of Layer 2 Frames Over MPLS", RFC 4906, DOI 10.17487/RFC4906, June 2007, <http://www.rfc-editor.org/info/rfc4906>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <http://www.rfc-editor.org/info/rfc5890>.

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, DOI 10.17487/RFC5891, August 2010, <http://www.rfc-editor.org/info/rfc5891>.

[RFC5892] Faltstrom, P., Ed., "The Unicode Code Points and Internationalized Domain Names for Applications (IDNA)", RFC 5892, DOI 10.17487/RFC5892, August 2010, <http://www.rfc-editor.org/info/rfc5892>.

[RFC5893] Alvestrand, H., Ed. and C. Karp, "Right-to-Left Scripts for Internationalized Domain Names for Applications (IDNA)", RFC 5893, DOI 10.17487/RFC5893, August 2010, <http://www.rfc-editor.org/info/rfc5893>.

[RFC5944] Perkins, C., Ed., "IP Mobility Support for IPv4, Revised", RFC 5944, DOI 10.17487/RFC5944, November 2010, <http://www.rfc-editor.org/info/rfc5944>.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <http://www.rfc-editor.org/info/rfc6120>.

[RFC6162] Turner, S., "Elliptic Curve Algorithms for Cryptographic Message Syntax (CMS) Asymmetric Key Package Content Type", RFC 6162, DOI 10.17487/RFC6162, April 2011, <http://www.rfc-editor.org/info/rfc6162>.

[RFC6783] Levine, J. and R. Gellens, "Mailing Lists and Non-ASCII Addresses", RFC 6783, DOI 10.17487/RFC6783, November 2012, <http://www.rfc-editor.org/info/rfc6783>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <http://www.rfc-editor.org/info/rfc6973>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <http://www.rfc-editor.org/info/rfc7230>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <http://www.rfc-editor.org/info/rfc7231>.

[RFC7232] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests", RFC 7232, DOI 10.17487/RFC7232, June 2014, <http://www.rfc-editor.org/info/rfc7232>.

[RFC7234] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Caching", RFC 7234, DOI 10.17487/RFC7234, June 2014, <http://www.rfc-editor.org/info/rfc7234>.

[RFC7235] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Authentication", RFC 7235, DOI 10.17487/RFC7235, June 2014, <http://www.rfc-editor.org/info/rfc7235>.

[RFC7236] Reschke, J., "Initial Hypertext Transfer Protocol (HTTP) Authentication Scheme Registrations", RFC 7236, DOI 10.17487/RFC7236, June 2014, <http://www.rfc-editor.org/info/rfc7236>.

[RFC7237] Reschke, J., "Initial Hypertext Transfer Protocol (HTTP) Method Registrations", RFC 7237, DOI 10.17487/RFC7237, June 2014, <http://www.rfc-editor.org/info/rfc7237>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

[RFC7626] Bortzmeyer, S., "DNS Privacy Considerations", RFC 7626, DOI 10.17487/RFC7626, August 2015, <http://www.rfc-editor.org/info/rfc7626>.

[Rideout] Rideout, A., "Making security easier", 2008, <http://gmailblog.blogspot.de/2008/07/making-security-easier.html>.

[RSF] RSF, ., "Syria using 34 Blue Coat Servers to spy on Internet users", 2013, <https://en.rsf.org/syria-syria-using-34-blue-coat-servers-23-05-2013,44664.html>.

[Sauter] Sauter, M., "The Coming Swarm", Bloomsbury, London , 2014.

[Schillace] Schillace, S., "Default https access for Gmail", 2010, <http://gmailblog.blogspot.de/2010/01/default-https-access-for-gmail.html>.

[Schneier] Schneier, B., "Attacking Tor - how the NSA targets users' online anonymity", 2013, <http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity>.

[spdy] The Chromium Project, "SPDY - An experimental protocol for a faster web", 2009, <https://www.chromium.org/spdy/spdy-whitepaper>.

[spiegel] SPIEGEL, "Prying Eyes - Inside the NSA's War on Internet Security", 2014, <http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html>.

[techyum] Violet, ., "Official - vb.ly Link Shortener Seized by Libyan Government", 2010, <http://techyum.com/2010/10/official-vb-ly-link-shortener-seized-by-libyan-government/>.

[torproject]
The Tor Project, ., "Tor Project - Anonymity Online", 2007, <https://www.torproject.org/>.

[torrentfreak1]
Van der Sar, E., "Proposal for research on human rights protocol considerations", 2015, <https://torrentfreak.com/is-your-isp-messing-with-bittorrent-traffic-find-out-140123/>.

[torrentfreak2]
Andy, ., "LAWYERS SENT 109,000 PIRACY THREATS IN GERMANY DURING 2013", 2014, <https://torrentfreak.com/lawyers-sent-109000-piracy-threats-in-germany-during-2013-140304/>.

[turkey] Akguel, M. and M. Kirlidoğ, "Internet censorship in Turkey", 2015, <http://policyreview.info/articles/analysis/internet-censorship-turkey>.

[UDHR] United Nations General Assembly, "The Universal Declaration of Human Rights", 1948, <http://www.un.org/en/documents/udhr/>.

[ververis]
Vasilis, V., Kargiotakis, G., Filasto, A., Fabian, B., and A. Alexandros, "Understanding Internet Censorship Policy - The Case of Greece", 2015, <https://www.usenix.org/system/files/conference/foci15/foci15-paper-ververis-update.pdf>.

[Walfish] Walfish, M., Stribling, J., Krohn, M., Balakrishnan, H., Morris, R., and S. Shenker, "Middleboxes No Longer Considered Harmful", 2004, <http://nms.csail.mit.edu/doa>.

[wikileaks]
Sladek, T. and E. Broese, "Market Survey - Detection & Filtering Solutions to Identify File Transfer of Copyright Protected Content for Warner Bros. and movielabs", 2011, <https://wikileaks.org/sony/docs/05/docs/Anti-Piracy/CDSA/EANTC-Survey-1.5-unsecured.pdf>.

[xmppmanifesto]
Saint-Andre, P. and . XMPP Operators, "A Public Statement Regarding Ubiquitous Encryption on the XMPP Network", 2014, <https://raw.githubusercontent.com/stpeter/manifesto/master/manifesto.txt>.

[Zuckerman]
Zuckerman, E., Roberts, H., McGrady, R., York, J., and J. Palfrey, "Report on Distributed Denial of Service (DDoS) Attacks", The Berkman Center for Internet and Society at Harvard University , 2010, <https://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_DDoS_Attacks_Human_Rights_and_Media.pdf>.

11.2. URIs

[1] mailto:node@domain/home

[2] mailto:node@domain/work

[3] mailto:hrpc@ietf.org

Authors' Addresses

Joana Varon
Coding Rights

EMail: joana@codingrights.org

Niels ten Oever
Article19

EMail: niels@article19.org

Claudio Guarnieri
Centre for Internet and Human Rights

EMail: nex@nex.sx

Will Scott
University of Washington

EMail: wrs@cs.washington.edu

Corinne Cath
Oxford Internet Institute

EMail: corinne.cath@oii.ox.ac.uk