Lindeberg, Fredrik

Conference Paper

How stable is the internet to malign or economic interference?

28th European Regional Conference of the International Telecommunications Society (ITS): “Competition and Regulation in the Information Age”, Passau, Germany, July 30 - August 2, 2017

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Lindeberg, Fredrik (2017) : How stable is the internet to malign or economic interference?, 28th European Regional Conference of the International Telecommunications Society (ITS): "Competition and Regulation in the Information Age", Passau, Germany, July 30 - August 2, 2017

This Version is available at:
http://hdl.handle.net/10419/169481

Terms of use:
Documents in EconStor may be saved and copied for your personal and scholarly purposes.
You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.
If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.
How stable is the internet to malign or economic interference?

Fredrik Lindeberg
Department of Management and Engineering, Linköping University

This text is a working paper on the social resilience of the Internet, which means who can change how we do end-to-end best effort digital communication and how can they change it. I assume a bottom up organized version of the Internet and focus on the Internet itself. The text goes through varying factors capable of through social means changing what the Internet is through intention or error, and concludes that a changing world order has the greatest impact on what the Internet will be in the future.

If we assume that the Internet is not strictly governed, but instead, along the lines of Zittrain (2008) and van Eeten and Mueller (2012), think that the Internet is more of construct with emergent qualities, governed by consensus and formed by day to day actions of its constituents (i.e. Internet-actors), then it is interesting to look at how sensitive this structure can be to external interference.

Practically, the Internet can be seen as a technical network, whose technical aspects in turn are managed by people. The area I explore is “how could someone disable the Internet?”, a question which is usually answered by technical means and has a vast flora of literature, for example Çetinkaya, Bryyles, Dandekar, Srinivasan, and Sterbenz (2013), Cohen, Erez, Ben-Avraham, and Havlin (2000), Rohrer, Jabbar, and Sterbenz (2014), Sterbenz et al. (2013), Wu, Zhang, Mao, and Shin (2007), Yuan, Zhang, Li, Zhang, and Li (2008) who all look at how the network itself can be disabled. I venture to ask the question if “someone” could disable or similarly incapacitate parts the Internet. I intend to explore these social vulnerabilities.

I use the term social resilience as an umbrella term for resilience to social changes and disruption in contrast to technical resilience. I initially planned to use social network theory, the theory of structural holes (Burt, 2004) and weak ties (Granovetter, 1973) to analyze and look for these potential “someones”, but ended with a qualitative overview instead.

Is it possible to disable or change the Internet by systematically targeting key people or by taking over an Internet-organization? I can think of two main goals of social disruption; disabling the Internet or controlling part of the Internet for political or economical reasons.

Could a terror group be interested in disabling the Internet? Could a commercial actor be interested in controlling or imposing tariffs on certain types of content?

1. How socially resilient is the Internet?
2. How can the Internet be disrupted through social means?

In this text I will assume that the reader has a working knowledge of organizations related to the Internet and Internet governance in general, and I will only introduce them shortly if at all. For a more coherent overview I recommend the empirical part of Lindeberg (2017). For avoidance of doubt, I am using an Internet ecology which is intentionally organized bottom-up.

Method

My initial plan was to create a network of important people in the Internet ecosystem, and use the theories of weak ties and structural holes to identify particularly interesting individuals or positions, but after conducting several interviews I realized that my approach was faulty, I had assumed that there were people in charge who directly could be influenced. As it turns out there are people with more influence than “average” but surprisingly few, and the Internet is not governed top-down which adds further issues to a weak ties and structural holes approach (Lindeberg, 2017).

This led me to reformulate my approach into a qualitative interview series with focus on social resilience. I would recommend a future researcher to try the structural holes and weak ties approach to Internet governance in the future, but to expect that a full network map would necessarily need to encompass almost all ICANN structures (such as the EC, ASO, GNSO, ccNSO, ALAC, SSAC, and RSSAC), ISO structures (such as IAB, IETF, IRTF), UN-structures (i.e. the ITU and committees), civil society (for example the connections of ALAC and EC), businesses (both infrastructure operators such as IXPs and ISPs but also digitization companies such as Microsoft, Google and Apple) and countries (governments and government bodies) (Lindeberg, 2017), due to the fact that the Internet is coordinated rather than governed (in the top-down sense of the word) (Lindeberg, 2017).

The interviews are limited due to the time frame of data collection, and is for all intents and purposes a starting point. The formal interviews were semi-structured and recorded and conducted in either English or Swedish, my native language. The interviews are in no way exhaustive but are a result of time and geography.
This text is dependent on data and results of a draft sent to this same conference, this text is referred to as Lindeberg (2017), and for avoidance of doubt, I am also the author of that paper.

Internet

As argued in Lindeberg (2017), defining the Internet is not easy and conclusions drawn will be heavily dependent on the definition used. I will here adopt the same Internet definition as in Lindeberg (2017), which is the Internet as a concept of end-to-end communication using pre-agreed upon standards for digital communication. In this definition the web is one service possible due to the Internet, another such service might be TV or radio over the Internet. The Internet is quite distinct from telecommunications in organization and regulation, in that the Internet is regulated through bottom-up processes whilst telecommunication is regulated top-down, even though telecommunication and the Internet occasionally might share the same infrastructure (Lindeberg, 2017).

In the scope of this paper it will limit me from looking at social means that might shape the usage of one particular service, such as the web, Facebook or Snapchat, but rather focus on social means shaping Internet itself and its development. Central functions are in effect limited to the IANA function and its constituents, which would be RIRs for numbering (i.e. AS-es and IP-address allocation) and ICANN for naming (i.e. allocation of TLDs in the DNS-system), and the information carriers themselves, such as ISPs and IXP.

I am in this text mixing the expressions Internet governance and Internet coordination which have the same meaning, although I will favor coordination since governance can be understood as there being a governor or an entity in need of governing.

This has the effect that one part of the research question roughly can be equated to how do can someone(s) disrupt or control the IANA function, whilst still ensuring that their IANA function is the one who’s coordination is trusted. And another part would be how the outcomes of the coordination is implemented, if at all.

IXP 1 (2017b) argues that the Internet works if everyone is doing their thing and their thing only, and it does not matter who actually does it, in the context of whether ISPs have to be private or could be government operated. This is part of the bottom up mentality of Internet coordination.

Multi-stakeholderism

ICANN has since they changed their bylaws in 2016 incorporated a multistakeholder approach in their governance model (ICANN, 2016a), with the Empowered Community (EC) as an oversight organization for some of ICANN’s functions (ICANN, 2017b). EC’s powers include but are not limited to recalling the board, selling ICANN assets and rewriting the ICANN bylaws. The EC is being described as a way for ICANN’s SOs and ACs to organize as a separate organization under California law (ICANN, 2017b), but the EC does not represent two ACs; Root Server System Advisory Committee (RSSAC) and Security and Stability Advisory Committee (Security and Stability Advisory Committee) (ICANN, 2017b, IXP 1, 2017b).

According to IXP 1 (2017b) much of the EC infrastructure is lacking appointees which would mean that an organized group could gain disproportional influence in the EC.

As described in Lindeberg (2017) the Internet can be seen as a semi-adhocratic organization with clear tendencies of process standardization here and there. This adhocratic structure is inherently harder to control and manipulate from one point, since most coordination is not formal in its character and there are usually not clear hierarchies (Mintzberg, 1993). This makes it hard for a coordinated take-over to happen, and even if such a take-over could theoretically happen there would be no purpose to it since you could just ignore them as long as they only control the coordinating organizations (ccTLD 1, 2017; IXP 1, 2017a).

IXP 1 (2017b) reasons that even though there is power in the coordination function, i.e. controlling ICANN, the processes themselves are slow and it would be possible for Internet actors to create a replacement organization before the over-taken controlling function could create long standing harm. For avoidance of doubt, the coordination function here is IANA, i.e. the coordination of IP-addresses, TLD-names and to some extent protocol specifications.

<table>
<thead>
<tr>
<th>Type of Organization</th>
<th>Role</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccTLD</td>
<td>Security officer</td>
<td>ccTLD 1 (2017)</td>
</tr>
<tr>
<td>ccTLD</td>
<td>Security officer and CEO</td>
<td>ccTLD 1 and ccTLD 2 (2017)</td>
</tr>
<tr>
<td>IXP</td>
<td>Research director</td>
<td>IXP 1 (2017a)</td>
</tr>
<tr>
<td>IXP</td>
<td>Research director</td>
<td>IXP 1 (2017b)</td>
</tr>
<tr>
<td>N/A</td>
<td>EU-politician</td>
<td>Politician 1 (2017)</td>
</tr>
</tbody>
</table>

Table 1

Formal interviews used in this paper
ICANN though is not the only organization of importance on the Internet, but they are quite central (Lindeberg, 2017), but as soon as we expand the scope we have ccTLDs, gTLDs, ISPs, IXPs, governments, businesses, academia, civil society etc who all have input into the EC and other vital parts of the Internet infrastructure.

It is worth noting that the Internet is intentionally bottom up, not just emergent bottom up because planning was non-existent, as can be seen in IETF (2012) and described by ccTLD 1 and ccTLD 2 (2017) and IXP 1 (2017a). There is a philosophy built in the Internet intentionally transcending nationality (IXP 1, 2017b) and organizing in a way different from governments (IETF, 2012) that should not be forgotten. Since the Internet is bottom up it is possible to just stop listening and electing a new coordinating entity if the current one should stop working in a direction favoured by its constituents (ccTLD 1 & ccTLD 2, 2017) IXP 1 (2017a), This makes the impact of the EC structure being infiltrated or taken over smaller, but not negligible.

The ICANN mission

Interestingly, some of the changes in the ICANN bylaws with regards to the IANA transition were not recognized during my interviews, which indicates that there is not wide recognition that the bylaws changed greatly in conjunction with the IANA stewardship transition, which further reinforces the picture that the bylaws changed greatly in conjunction with the interviews, which indicates that there is not wide recognition that the bylaws changed greatly in conjunction with the IANA stewardship transition, which further reinforces the picture that ICANN is not seen as that important by Internet organizations. Historically ICANN has revised or amended their bylaws on average twice a year, with two major revisions so far: a rewrite in 2002 and a large amendment in conjunction with the IANA stewardship transition in 2016 (ICANN, 2017a).

In 2002 most of the bylaws were rewritten and a mission statement was added saying “The mission of The Internet Corporation for Assigned Names and Numbers ("ICANN") is to coordinate, at the overall level, the global Internet’s systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet’s unique identifier systems” (ICANN, 2002). Prior to that rewrite the bylaws did not contain a mission statement. In the 2016 amendments the mission statement was altered to “The mission of the Internet Corporation for Assigned Names and Numbers ("ICANN") is to ensure the stable and secure operation of the Internet’s unique identifier systems as described in this Section 1.1(a) (the "Mission")" (ICANN, 2016a), and with that removing the limit of ICANN only coordinating as their main mission, but rather being given greater leeway in terms of possible actions within their bylaw mandate.

Another important difference in ICANN’s bylaws is that ICANN now has in their mission to collaborate with other bodies as appropriate (ICANN, 2016a), even though the by-laws limits ICANN’s mandate to collaboration, rather than say, signing treaties (ICANN, 2016a).

In the short term these changes are not going to change how the Internet functions, but long term the purpose of ICANN could change, especially given the fact that there is a political and legislative need for a formal Internet governor.

Human error

ccTLD 1 (2017) mentioned that the root zone file has been close to being corrupted a couple of times due to human error. In general human error is not something that could be discounted as having an influence on the stability of the Internet, especially as a bottom up approach to organizing in general leaves room for mistakes since there are no strict processes in place.

In general organizational terms adhocratic constellations are more dependent on people than stricter standards based organizations who in turn are more dependent on a valid standardization process (Mintzberg, 1995).

I can not in my interviews find any long term threats to the Internet as it is or its development coming from human error.

BIND

Most of the root servers use BIND (Wikipedia Contributors, 2017), an open source DNS software for DNS servers. ccTLD 1 (2017) explained that it would be problematic if the software no longer could be trusted. BIND is currently developed by Internet Systems Consortium (ISC) through an open source process (ISC, 2017), and this process is considered secure enough by many (ccTLD 1, 2017).

With DNSSEC taking into account it would on the one hand be hard to spoof correct domains, but on the other hand easy to return garbage in RRSIG and DNSKEY fields of a DNS request thereby making the resolved host seem fake or spoofed, given the DNSSEC description (Arends, Austein, Larson, Massey, & Rose, 2005a[2005b][2005c] Hubert, 2017).

Reasonably it would be problematic if BIND was compromised but the software could reasonably easy be rolled back to an safe version if this happens and is noticed, but I imagine that a compromised BIND could cause quite a ruckus with regards to DNSSEC until resolved.

Politics

One of the interviews with IXP 1 turned into a foray of international politics and how different world orders are in
competition today. IXP 1 (2017b) describes that there are
two primary world views in conflict today, one promoting an
order with coordinated legislation across countries and na-
tions, and another promoting country sovereignty, and IXP
1 (2017b) admits being biased towards a coordinated leg-
islation. A coordinated legislation would by necessity require
some coordinating function, like the UN.

Politician 1 (2017) in a way agrees with IXP 1 (2017b),
but goes further in arguing that ICANN probably should be
placed under the UN. IXP 1 (2017a) does not think it is in-
herently wrong to have the IANA function (i.e. ICANN)
under a democratic organization, but thinks the UN is problematic
since all members states are not democratic nor in favour of
a coordinated world order, which the Internet inherently is in
favour for (ccTLD 1, 2017; IXP 1, 2017a).

In the context of politics and the UN both IXP 1 (2017a)
and ccTLD 1 and ccTLD 2 (2017) mentions that ICANN is a
good placeholder for the IANA function, since if ICANN did
not exist another organization would become the administra-
tive seat of IANA, and the IANA function could potentially
fall into the wrong hands.

As mentioned before IXP 1 (2017b) sees the most serious
threat to the Internet being a sovereign world order prioritiz-
ing national interests over international ones, since this over
time drastically could change the possibilities of having the
Internet or an Internet. Companies taking a big role in the
Internet coordination or controlling large parts of a commu-
nications chain, as described in Zittrain (2008), is described
as just bumps on the road by IXP 1 (2017a), as the same was
said about Yahoo and AOL previously.

IXP 1 (2017b) reasons that the only power large enough to
disrupt the Internet in a long term perspective are states giv-
ing in on the coordinated world order and rather focus on
their own sovereign.

ISP and IXPs

As argued in Lindeberg (2017) ISPs, and to a lesser extent
IXPs, have the power to shape what the Internet is for the
end user. One power keeping ISPs and IXPs in check is legis-
lation which could regulate to which extent traffic can be
modified or logged.

It seems natural to assume, since ISPs in general are com-
ercial wholesalers, that they want to use their competitive
advantage to its fullest, and provide their own services
rather than a general distribution service. For example an
ISP might be more interested in selling their own streaming
service rather than a general Internet based service such as
Netflix.

Although as long as there is regulation in place ensuring
that no packet filtering or other such activity takes place this
should not be a major concern for the future. The business
end of packet filtering is usually referred to as net neutrality,
and in essence often concern particular services.

IXP 1 (2017b) believes that this horizontal vs vertical inte-
gration is going to be an issue for the future, since the In-
ett only works if everyone does what they are supposed
to do, and actors like Facebook changes how services are
available since some services are available only for Facebook
users. This is problematic since everyone who has access to
the Internet does not have access to Facebook.

One issue with both ISPs and IXPs is that regulation is of-
ten not appropriate with regards to how the Internet works.
The Internet is a best effort based packet switching network,
which is different from specialized services as is common in
telecommunications (IXP 1, 2017b). As an example there
has recently been a push towards traffic priority for Public
Protection and Disaster Relief (PPDR) which is problematic
since it would require a change in how routing and packet
forwarding works (IXP 1, 2017b), and even getting into the
area of net neutrality.

The problem being that there is a push from a regulatory
perspective to make the Internet into something which can be
regulated, rather than the unintentionally unregulated coor-
dination of standards and practices it is today.

Conclusions

In its base form, i.e. as a means of end to end digital com-
unication, the Internet is quite resilient, but it can be seen
as troublesome that the EC has a number of vacancies which
could be used to push policy through ICANN. Although this
would only have long standing effect as long as the world
outside of the Internet ecosystem considers ICANN as a ne-
gotiator for all things Internet since the Internet actors them-
selves usually are quite clear that they are not contractually
bound to ICANN. But since the bylaws for ICANN offer a
greater leeway now than earlier for negotiating and collabo-
rating with other organizations this possibility should not be
discounted.

With that said I argue on the one hand, the short term, that
the social resilience of the Internet is high in that no con-
stellation of people or organizations in a short time frame
could redefine what the Internet is. But on the other hand
there are long term pressures which could possibly change
how the Internet is organized and coordinated. For example
the bylaws of ICANN has changed from being explicitly
coordinating in it’s mission in ICANN (2016b) to dropping
the explicit coordinating in ICANN (2016a) and rather focus
on ensuring a secure and stable operation of central Internet
functions. Not to be forgotten is that the Internet given that it is the possibility of end-to-end communication using agreed upon standards by the users, stops being the Internet as soon as it is regulated rather than coordinated.

The reason for the Internet’s base resistance is that coordination is based on mutual acknowledgements, i.e. that powers in some sense only exist if recognized and no central authority exists, and that if malicious actors appear they can be ignored. Even if someone assumes the power in ICANN it should be possible to reorganize basic Internet coordination in another forum, although ICANN possibly retain its political standing with non Internet actors which would create long term issues as just mentioned.

Neither should BIND nor other Internet infrastructure essential software be considered non-problematic since it might be possible to manipulate the software to serve someone’s purposes.

To answer the initial research questions in an orderly fashion:

1. How socially resilient is the Internet?
   The Internet is very socially resilient.

2. How can the Internet be disrupted through social means?
   Short term, vacancies in the EC structure. Long term, political pressure towards national interests and regulation rather than international collaboration and coordination.

The future of the Internet should not be taken for granted with the forces we have in play today, but the Internet cannot be changed overnight.

References


