Steering Committee on Media and Information Society (CDMSI)

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

CDMSI(2013)misc 20

5th meeting
Strasbourg, 3-6 December 2013

Consolidated report on the cross-border flow of Internet traffic and interference which may have an impact on access to content, services and applications

Report prepared from a technical and a legal perspective, in the context of Article 10 ECHR (the right to freedom of expression)

By Dr Monica HORTEN
Visiting Fellow at the London School of Economics & Political Science

From three original reports by
Professor Yaman Akdeniz, Istanbul Bilgi University
Patrik Fältström, Chair of the Security and Stability Advisory Committee, ICANN
Professor Michael Rotert, University of Karlsruhe, Honorary Spokesperson EuroISPA

The authors wish to acknowledge the kind assistance of Joanna Kulezsa, Assistant Professor at University of Lodz, Paul Fehlinger, Manager Internet & Jurisdiction Project, and the extensive contribution of Gordon Lennox, former member of the European Commission, DG Information Society and Media.

Table of Contents

Introduction

The Council of Europe is concerned with the possibility of interference with Internet content across borders. The concern is with interference with parts of the infrastructure of the Internet, specifically with the traffic routing, and at the interface between the network and the content, that affects Internet users' ability to access or provide content and services. The concern is not just with accidents or security incidents, but with actions to block, filter, divert or intercept content in one Member State, that may impact on users who are based in another Member State. Such actions may be politically driven by State and other public-sector actors, but importantly, they may also be commercially driven by private-sector actors.

This report considers methods of blocking, filtering, redirection or surveillance that may be used in this context. In particular, it addresses how these methods utilise the technical infrastructure of the Internet to limit or constrain the provision of content and access to it, and how such methods frequently result in non-targeted, legitimate content being affected. The report addresses the possible motivations of State and commercial actors for implementing such policies, and it examines the possible cross-border effects. Taking each of the blocking methods one by one, it relates known incidences, and it proposes scenarios to illustrate how such blocking methods can create cross-border effects. The report then gives an overview of the likely legal position - 'likely' because no case law currently exists.

Finally, the report provides recommendations regarding elements that could be included in an Instrument to address the cross-border flow of Internet traffic and interference with both the offer of content and access to it, and a further recommendation to consider an Instrument to address mass scale surveillance of traffic, in terms of its content and metadata, as recently uncovered with the revelations on the Prism and Tempora projects.

This report builds on the work done in the Council of Europe Recommendation of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet[1] which addresses the resilience and resource management of the Internet infrastructure, and is concerned in particular with the possibility of accidents or security incidents and their possible impact on cross-border traffic flows. The 2011/8 Recommendation stated that the right to freedom of expression applies regardless of frontiers, and that freedom of expression depends on actions related to the infrastructure. It set out three principles: no harm, co-operation and due diligence. States should ensure that their actions do not have an adverse transboundary impact on access to and use of the Internet. They should co-operate to prevent such an adverse transboundary impact, and take all necessary measures to prevent it.

The *2011/8 Recommendation* is also concerned with promoting good governance of the Internet, in particular with regard to the Domain Name System. The *2011/8 Recommendation* makes no assumptions regarding the application layer and content (see below – Layered Structure of the Internet). It is therefore a logical progression from the *2011/8 Recommendation* to address how interference at different levels of the network infrastructure may interfere with access to content.

This report further builds on the Preliminary Report on scenarios of interference with Internet traffic which may have an impact on access to information across borders[2] of the Steering Committee on Media and Information Society. This Preliminary Report[3] found that 'Internet traffic in one country

[1] CM/Rec(2011)8

[2] CDMSI (2012)015

[3] P2

may be exposed to undue interference by other countries or to actions taking place within their jurisdictions– e.g. country A or action taking place within that country may have an impact on the Internet traffic in country B. This may result in cross-border implications for access to content and information carried by that traffic.' It incorporated a reminder that 'under the European Convention on Human Rights (ECHR) states have the obligation to secure to everyone under their jurisdiction the protection of the right to freedom of expression, including the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers (Article 10 of the ECHR).'

This report is compiled using three expert reports commissioned for the Council of Europe: CoE Cross Border Report, prepared by Professor Yaman Akdeniz;[4] Incidents Affecting cross border flow of Internet traffic, prepared by Professor Michael Rotert; and Report on the free cross-border flow of Internet Traffic, prepared by Patrik Fältström[5]. In particular, the legal analysis of Professor Akdeniz has been incorporated in a substantial part. Additional sources include the Guardian, Open Network Initiative, and other media reports and case law as relevant.

Interference with access to content

One very important point to understand for the purposes of this report is what constitutes interference for the purposes of Article 10 of the Convention. In order to achieve that understanding, it is necessary to look at how the Internet functions from a technical viewpoint. It should be noted that Article 10 is a two-way right to receive and to impart information without interference, and this report is concerned with interference that may occur to both elements of the Convention right.

Internet traffic is not routed directly from one point to the other. This is what makes it different from, for example, an old-style telephone network. On a traditional telephone network, the connection would be made directly between two telephones using switches to connect physical wires and the transmission of the voice signal would run point-to-point over a fixed wire from one user to the other. Any interference with the communication would therefore have to be targeted and specific to the individuals at either end of the line.

On the Internet, there is no such direct connection between the user and the website he is talking to. Instead, the data is broken up and put into packets, which are marked with an 'address' and find their own way around the network. At their destination, they are re-compiled to give the user the data – such a webpage – in a form that he understands. Two packets from the same logical connection may travel by two very different routes and be re-compiled at the other end. Those packets will be intermingled with packets from many other transactions involving many other parties.

This means when an Internet user views a web page, there is no physical connection between the user's computer and the server from which the data has come. The user's computer has merely sent a request to view the page, and server has responded by sending the data, which is re-compiled on the user's computer for display on the screen. Any interference has to utilise the various elements of the network and the more targeted it is, the deeper it may have to interfere. Moreover, because the interference works by instrumentalising different parts of the network, there is a strong chance that there will also be interference with content that is not targeted. This section will explore these notions by considering the layered structure of the Internet, how a 'borderless' network can be controlled within borders, and different technical forms of interference.

[4] Faculty of Law, Istanbul Bilgi University, Turkey.
[5] These will be referred to in the text and will be cited as either Akdeniz, or Rotert, or Fältström.

The layered structure of the Internet

The Internet should not be thought of as a single entity. Instead, it should be regarded as a set of layers. In very simplified terms, those layers provide clearly identifiable functions[6] that are critical to the operation of the network.

At the very top of the network is the actual content[7], which is the part that most of us think of as 'the Internet' – this is the visible part, that we understand using human intelligence - the website text, the services such as Skype and Google, the colour, the images, the videos and audio. The content is the part that concerns the Convention Rights enshrined in Article 10 to receive and impart information without interference. This report is interested in how interference with any of the layers in the network may affect the ability to view and access that content, and conversely, how a deliberate intention to interfere with content will require action to be taken within those network layers.

The top layers[8] - known as the application and presentation layers - act as a go-between for a website and the network beneath it, carrying requests between the two, and ensuring that the correct processes are established. The application layer also provides the means for the data to be displayed on people's computer screens. The many different applications and services that we are familiar with are found here, including the ones that control access to email and websites, as well as those that carry out and run streaming, gaming, Internet radio and television, chat, messaging, Internet telephony and file transfer. Others, such as the DNS, are invisible to the user.

The middle layers, known collectively as the IP layer,[9] provide the routing mechanisms that organise the packets of data, tell them where to go and transmit them. The packets consist of a header (the source and destination addresses) and the payload (the data of interest to applications). Intermediate computers (or routers) simply look at the header and forward the packet as appropriate. This will normally be repeated many times until the packet reaches its destination where the packet will be passed up to the next layer. This means that the physical links do not have to be concerned by the applications or content. At the same time the application and presentation layers can ignore the characteristics of the physical links. The IP layer interfaces to the application layer and to the physical layer.

The physical layer is the lowest one, comprising the wires and cables that carry the electronic signals encoding the data to be transmitted, These cables include such things as the Ethernet cable you may use at home or in the office and long-distance under-sea optical cables. The physical layer also includes wireless links such as WiFi and mobile phone and satellite links. Internet communications will involve various technologies depending on the individual links. So a laptop will be connected wirelessly to a WiFi base-station which will in turn be connected via an Ethernet cable to a modem. Data travelling to and from the laptop may be transmitted via an optical cable under the ocean.

---

[6] For the purposes of explaining how the Internet works to a non-technical reader, the network model has been simplified in this account.

[7] In strict technical terms, the content does not count as a layer of the network – instead, it is considered something which sits on top of the network layers.

[8] Technically the application and presentation layers; also referred to as the *service layer*.

[9] Technically, the data link, network, transport and session layers; also referred to as the *IP layer*

How a 'borderless' network can be controlled within borders

The original aim of designing the network in this way was to ensure that it would be resilient against an attack.[10] In meeting that aim, it was important that the overall network would not be dependent on any particular connection or server for its continued operation, such that if one server or link was unavailable for any reason, the traffic would continue to run via the other connections and servers.

Hence, the IP layer of the Internet was designed to send traffic using a dynamic system that is able to use a variety of different routes between any two points. This means that there is no central point that controls the entire network, and no one individual person, State or organisation owns it. The data finds its way around the network by means of addressing information that is put on the packets by the computers that are to communicate.

In this sense, the Internet is often considered to be 'borderless' because the network traffic is not routinely stopped at borders and it ignores the existence of borders. The perception of the Internet as a 'borderless' network may also be due to the ability to access content and services from other States and across national borders.

However, when looked at from a different perspective, this perception of the borderless network is actually false. The physical infrastructure of the Internet including the cables, wires, devices, signalling equipment, servers and the routing mechanisms, is almost entirely located within territorial jurisdictions[11]. It is this equipment which States may control and which provides the means for them to exercise controls over the other layers, including the content layer[12]. This applies even when the infrastructure is owned and operated by commercial actors such as Internet service providers and telecoms companies, because States may exercise control via regulation

Taking this perspective, the Internet - namely infrastructure owners, service providers, other intermediaries and users - does have to comply with the law in the jurisdictions in which it operates, and it can be governed by it. The 'interference' with content that is the subject of this report, is interference applied within jurisdictions.

Interference with content

In the context of this dynamically-routed, layered network structure, 'interference' therefore does not mean a simple action to block a direct connection between two computers. It cannot mean this, as there is no such connection.

Instead it means a more sophisticated technical action ordering changes with application layer, including the domain name system, or with the routing or the addressing systems, in order to prevent the system from successfully fulfilling the user's request to view a webpage or use an application.

Blocking may be carried out by interfering with the application layer. For example, requests for individual web pages or URLs[13] may be redirected to an alternative web-site or simply discarded. Blocking may also be effected by targeting entire groups of applications such as those using peer-to-peer or gaming protocols. Similarly, blocks can also be implemented by interfering with the routing functions in the IP layer, for example, by compiling blacklists of IP addresses.

---

[10] The original Internet design was commissioned by the US Defense Department for military purposes. The Internet was opened up to commercial users in 1992.

[11] The exception being undersea cables that run beyond the 12 mile limit, and some satellite equipment.

[12] For a longer discussion, see Goldsmith and Wu, 2006, Who Controls the Internet? Illusions of a borderless world, Oxford University Press.

[13] Universal resource locator

Another method of blocking is to use the Domain Name System[14] by removing a domain name from the authoritative servers. Typically, this will happen when a domain is 'seized' by the authorities. DNS blocking may also be implemented by programming some name servers not to resolve (or answer requests for) a certain page.

'Blocking' may also take the form of removal of content by a hosting or platform provider. This may be a company that hosts multiple websites (hosting provider), or that offers a facility for others to upload their own content (platform provider). The latter include video hosting sites such as YouTube, blogging sites such as Blogspot.com, and social media sites such as Twitter. The removal may be preceded by a notification, in which case it is referred to as 'notice and take-down'. In a more extreme form, it may entail the seizure of the server itself and the data it holds.[15] Alternatively, it may entail the removal of certain essential facilities, such as payment facilities, from a user's account. In this case, the actual content is not blocked, but the provider's ability to continue the service may be impacted by the removal of finance, and the *de facto* outcome is the removal of the content.

An important concept is that of 'overblocking'. For example, if the filter or block is not absolutely specific to the content that is to be barred, then other content, which is legitimate and not subject to the order, may also find itself blocked. The case of *Yildirim v. Turkey* provides an example where a block ordered against one particular site on Google Sites had the effect of blocking access to other sites which did not infringe any law and were legitimate. The case concerned a challenge to that block by the owner of one of the affected sites. [16]

Overblocking may also be a consequence of targeting domains through the DNS:

> "it is important to recognize that if blocking is implemented for a domain such as example.com, blocking using the domain name system will not only block the ability to look up the domain name when accessing content under the blocked URL http://example.com/bad-content.html, but also all other URLs using that same domain name; e.g., under http://abc.example.com/ or http://example.com/good-content.html. DNS blocking will also block domain name lookup for all other services such as e-mail, network management, file transfer, etc. that use the same domain, and additionally, child domains of example.com (e.g., subdomain.example.com)."[17]

It's also interesting to note that asking Internet service providers to block large numbers of URLs, may cause other unintended consequences that could engage Article 10. For example, experience in Australia found that implementing a blocking list of more than 15000 entries may cause interference with traffic and bandwidth availability, because of the sheer volume of re-routing of the requests and the time it takes to carry out the lookup procedures.

Cross-border effects of interference with access to content

From the perspective of cross-border Internet, the concern is how such forms of interference could have an impact in another jurisdiction. This section provides examples of situations where cross-border interference with access to the Internet and web content has been experienced. The examples are drawn from a range of sources, including media reports, and do not, in the main, reflect legal

[14] DNS is both a naming system and an application layer protocol - see Patrik Fältström, Report for the Council of Europe on the free cross-border flow of Internet traffic, p12

[15] The case of MegaUpload is an example of where the server was seized.

[16] The case of *Ahmet Yildirim v. Turkey*, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013 (final) provides an example where a block ordered on Google Sites had the effect of blocking

[17] SSAC Advisory on Impacts of Content Blocking via the Domain Name System, SAC056, 09 October 2012 at http://www.icann.org/en/groups/ssac/documents/sac-056-en.pdf From Akdeniz, p11.

judgements. The section begins with a brief overview of the actors – political and commercial. It moves on to discuss the type of interference addressed by the 2011/8 Recommendation, followed by an examination of interference in the present context.

State and private-sector actors

Many of the examples cited below reflect situations where political actors, which may be States or government agencies, have imposed restrictions such as filtering or blocking, or some other interference with Internet traffic flow intercepting it for surveillance. In these cases, it would seem that the motive is purely to serve the perceived political interests of the State, whether international or domestic.

Private sector actors with commercial motives may collude or cooperate with political actors who want to restrict access to content, or to conduct surveillance on it. Such co-operation may be prescribed by law, as in the French Creation and Internet law (often referred to as the Hadopi law), or it may implemented by agreement, or voluntary co-operation. There is a tendency for such voluntary agreements to be encouraged and overseen by States, as in the US 6-strikes agreement for copyright enforcement.

The 2013 revelations concerning the Prism and Tempora projects by the US and the British intelligence services illustrate other ways in which commercial actors might co-operate with political actors in this context. Similarly, the removal of payment facilities from the Wikileaks website, and the seizure of its domain names represent another example of such collusion between commercial interests and the State to serve government interests. It is interesting to note that the IP address for the Wikileaks server was replaced by a website from the FBI, via a change in the top level domain files.

A relatively new phenomenon is that of the State asking private actors to implement restrictions that serve social policy goals such as children's access to web content or online gambling. It is unclear how this will impact on cross-border Internet access to content, however, where those commercial actors offer services across more than one jurisdiction, it may be that States will have to defend the rights of their citizens against commercially-motivated actors based outside their jurisdiction who are implementing policy of another State. It may also be the case that some commercial actors will be themselves affected by differing regimes of restrictions implemented by different States, for example, providers of cloud computing services or mobile roaming. The implications of this in the context of ECHR Article 10 are not yet clear, and could warrant further research.

It is worth noting however, that private actors may have their own motives to implement restrictions on access to the content. For example, they may be motivated by a desire to protect their business or address competition, in blocking certain application/content layer services such as voice over IP or video streaming. This will present a new situation from the viewpoint of human rights law, since the Convention is predicated on interference by a 'public authority' and the thinking behind it is likely to have been to protect against the possibility of political interference. In this new context, States may have to defend the Convention right to freedom of expression against commercial actors which be based outside their own jurisdiction.

The role of private actors in respect of rights within the cross-border Internet context could therefore become as crucial as that of States. In this context, it is noted that there is a proposal to permit telecoms operators from any European Union Member State to operate in another EU Member State under a single authorisation[18].

[18] A draft of the European Commission's proposed new telecoms regulation leaked in June 2013. It was made available at http://edri.org/files/consolidateddraft-ISC070713.pdf

Resilience and resource management as addressed by the 2011/8 Recommendation

The Recommendation of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet (2011/8) was primarily concerned with protecting the resilience of the network, as a means of ensuring the flow of data on the network, and thereby protecting the means of freedom of expression in the digital era.

The presumption was that resilience could be challenged by natural phenomenon such as earthquakes, fires, floods and acts of God, which can cause damage to the cables and the wires, microwave dishes, transmission equipment and the attached hardware and servers. The Internet is also vulnerable to deliberate acts of sabotage, either to its own physical infrastructure or to that of other utilities. For example, it is vulnerable to the deliberate cutting of telecoms cables or jamming of signals, as well as to attacks on power plants or water supply companies.

Where several States rely on the same infrastructure, there can be cross-border consequences. For example, in 2006, an earthquake off the coast of Taiwan broke a number of submarine cables, disrupting Internet traffic to and from several Asian countries including Taiwan, the Philippines, Malaysia and China. In 2007, when a San Francisco data centre lost power, it took down a number of major websites such as Craig's List, Live Journal and Second Life, for a period of several hours.[19]

The other concern of *Recommendation 2011/8* was security incidents. There have been a number of reported incidents where cross-border virus, worms and malware have resulted in websites being disabled or rendered inaccessible. For example, in 2001, the Code Red worm infected websites running Microsoft's IIS web server. The infected websites were tracked throughout North America, Europe and Asia, hence the example illustrates how computer viruses have a cross-border impact. In 2000, a series of DDOS attacks disabled several of the large websites such as Yahoo, CNN, Amazon and eBay[20]. A more recent example was the DDOS attack on the European Parliament website and on certain Polish government websites as a protest against a proposed copyright treaty known as the Anti-counterfeiting Trade Agreement (ACTA).

A possible issue for the Council of Europe when considering viruses and DDOS attacks in this context will be the motivation of the attackers, and whether the motivation is criminal – for example, to take control of servers for their own purposes - or whether it could be regarded as some form of political speech - for example, when accompanied by a public political statement. It is unclear at present if this is the case, and if so, how it should be treated. This issue is not addressed further in this report, but could be a subject for further analysis.

Interference with content via upstream filtering

Any new Instrument proposed by the Council of Europe would build on *Recommendation 2011/8* to address forms of interference in the others of the network that may affect access to content. One area to address is upstream filtering. This is a term used where the filtering or blocking implemented in one jurisdiction can have an effect in another jurisdiction as a direct consequence of Internet service provider routing arrangements. In a cross-border context, it can occur where an ISP whose primary location is in one jurisdiction, takes on as a secondary activity the supply of services to customers in another jurisdiction, without altering the blocking policy. Using the analogy of a river, the blocking occurs 'upstream' in the ISPs primary business, but flows downstream into the secondary activities. Hence, the Internet users in the secondary jurisdiction are deprived of access to content that may not necessarily be subject to any restrictions in their country, and in this context, there could be an issue under Article 10 ECHR.

[19] Both examples, Rotert, pp6-7

[20] Rotert, p6

There are a number of reported examples of the cross-border effects of upstream filtering; however, there is no case law. In 2009, the OpenNet Initiative found that a number of websites, including news sites and blogging platforms, were inaccessible in Kyrgyzstan. It was reported that the inaccessibility was a result of blocking by the state ISP in Kazakhstan, which sells its service to KyrgyzTelecom [21]. In 2004, the OpenNet Initiative had observed similar behaviour in Uzbekistan where content filtering on one Uzbek ISP closely matched that seen in China, a finding supplemented by evidence that this ISP was purchasing connectivity service from China Telecom.[22] More recently, in 2012, the Citizen Lab at the University of Toronto published research that showed that web filtering applied by India-based ISPs is restricting access to content for customers of an ISP in Oman.[23]

Interference due to error in network routing

Another form of interference that a new instrument could address concerns errors in the 'routing layer' (see above). In this layer, Internet Service Providers (ISPs) rely on information provided by other ISPs regarding the most cost-efficient route for the data packets to reach their destination. ISPs usually trust the information provided by other ISPs to be correct. However, routing information can be altered to announce diverts and to send traffic away from specific destinations. The same routing techniques can be used to give instructions for traffic requests to be discarded or delivered to an alternative destination such as a police notice that can be shown to the end-user. Therefore, the 'routing layer' of the Internet can be used to *de facto* block traffic.

There are some reported examples of how announcements by an ISP of changes to routing information can propagate on an international scale and affect access to specific content or services across borders. One example occurred on 22 February 2008, when an order by the authorities in Pakistan to block YouTube resulted in routing errors which for a short time blocked access to the video streaming site worldwide[24]. In 2004, a Turkish ISP (TT Net) made a mistake when configuring its routers, effectively announcing to the rest of the Internet that everything should be routed to them. The configuration error spread and resulted in tens of thousands of networks on the Internet sending traffic to the wrong destination.

In April 2010, China Telecom advertised incorrect traffic routes to the rest of the Internet. In this specific case it meant that during 18 minutes, potentially as much as 15% of the traffic on the Internet was sent via China because the routers believed it was the most effective route to take. Incidents such as this pose the risk that the whole network crashes since the ISP can't handle the traffic. However, China Telecom was able to handle the traffic, so the impact was minimal. It is thought that Internet users would have noticed nothing more than increased latency as traffic was slowed down. [25]

Where such incidents involve a genuine technical error, it may also be possible to resolve them at a technical level. Networks can also decide in the end who to accept announcements from. However, where the routing changes are made in order to implement a policy (whether or State policy or commercial), the implications for interference with access to content may engage the Article 10 Convention rights. The cross-border effect would seem to be similar to upstream filtering, in that the blocking action occurs 'upstream' and the effect is felt in another state that exists 'downstream'.

---

[21] See OpenNet Initiative, "Kyrgyzstan," (2010) at http://opennet.net/sites/opennet.net/files/ONI_Kyrgyzstan_2010.pdf

[22] See OpenNet Initiative, "Internet filtering in the Commonwealth of Independent States 2006-2007" (updated in 2010) at http://opennet.net/sites/opennet.net/files/ONI_CIS_2010.pdf

[23] See The Citizen Lab, University of Toronto, "Routing Gone Wild: Documenting upstream filtering in Oman via India," 12 July, 2012, at https://citizenlab.org/wp-content/uploads/2012/07/08-2012-routinggonewild.pdf

[24] Open Net Initiative, YouTube Censored : a recent history https://opennet.net/youtube-censored-a-recent-history Accessed 26 August 2013

[25] Rotert p 8; Akdeniz p4

Interference with the DNS

A new instrument would consider how the Domain Name System (DNS) could be altered in some places to create interference with content. The DNS provides the translation between domain names such as www.coe.int, and the IP addresses of the servers on the Internet. The DNS system can be used to block access to content by modifying the entries with the databases on name servers operated by registries. Alternatively, intermediate name servers can be programmed not to resolve a particular query (that is, not to tell the requesting computer which server the content is on). Some experts suggest that this form of blocking is quite common. Alternatively, the domain name of a website can be removed from the database altogether[26]. The cross-border effect of altering the DNS can be similar to that of upstream filtering in terms of the interference with access to content.

One incident, where a cross-border effect due to alteration of the DNS database was reported, was the case in 2010 of the whistle blowing website Wikileaks. Its DNS provider, EveryDNS, shut down its domain. Without a working domain in place, Wikileaks was effectively lost on the Internet. It could only be reached by those who knew its IP address[27] and users internationally were prevented from accessing its content. This restriction was imposed irrespective of whether it was or was not legal in the user's jurisdiction to access this content, and arguably would reflect an infringement of Article 10 ECHR in this context.

Another reported incident of cross-border interference with the DNS came in 2012, when the United States Department of Homeland Security seized a domain name registered in the US, through an accredited Canadian registrar, by Canadian citizens[28] and thereby blocked the operation of a Canadian-owned service. In 2010, the United States government seized the domain of the British-based site TV Shack, on the grounds that it was allegedly infringing copyright[29.] Another interesting example in the cross-border context is that of the Spanish website Rojadirecta. In this case, the domain was bought via a US-based registrar, and was seized by the US authorities, even though the website was deemed not to be illegal by a Spanish court.

Leveraging intermediaries

There is a growing list of instances where intermediaries such as hosting and platform providers, payment providers and Internet service providers, are being asked to block or take some other action to remove content. These requests include many that will have a cross-border effect. For example, US-based hosting platforms receive thousands of requests from private actors to remove content on the basis of copyright infringement, defamation and law enforcement issues[30]. In 2010, the United States government ordered that online payment facilities used by the website Wikileaks should be stopped. PayPal, Visa and MasterCard all stopped providing payment facilities. The website relied on donations and this action had the effect of severely restricting the ability of the website to seek funding, even though its main hosting platform was in Switzerland. There are also cases recorded of payment facilities to providers of virtual private networks (vpn) being stopped by credit card companies[31].

---

[26] Fältström , pp15, 17-18

[27] Rotert, p8

[28] US shuts down Canadian gambling site with Verisign's help, in The Register, http://www.theregister.co.uk/2012/03/01/bodog_shut_via_verisign/ Accessed 23 August 2013.

[29] 13 January 2012. Ruling: In the Westminster Magistrates Court. The government of the United States of America v Richard O'Dwyer

[30] For one example, see Google Transparency reports available on the Google website

[31] MasterCard and Visa start banning VPN providers. In Torrent Freak, 3 July 2013. http://torrentfreak.com/mastercard-and-visa-start-banning-vpn-providers-130703/

In another instance, the servers running a website were themselves targeted, when the US authorities seized servers for the cyber-locker service Megaupload. A cross-border effect occurred because service was legally based in Hong Kong, and operated by a German citizen who was a resident in New Zealand.

The so-called 'kill switch'

The 'kill switch' refers to the order by a State to cut off all Internet services within its jurisdiction or part of its jurisdiction. It can involve the selective closing down of local networks, especially mobile networks, or cutting off international connections. The latter is most easily applied where there is only a small number of an international Internet connection taking traffic outside the State borders and where those connections occur at or near the geographic border. An example comes from China in 2009, where the Chinese State blocked all outside Internet access to Xinjiang province for a period of more than 10 months[32]. In another example, Syria was cut off from the Internet for a period of some 19 hours on 7 May 2013. It has been suggested that this was a case of the Syrian government pulling the kill switch[33].

Azerbaijan has a law stating that under certain circumstances of national emergency, war, natural disasters of catastrophes, Internet services may be suspended[34]. The issue for cross-border effects is whether the 'kill switch' also kills or restricts Internet services for users in other jurisdictions. For example, what would be the effect if there were service or content providers in that jurisdiction who supplying users in other jurisdictions? It is notable, however, that the 'kill switch' action does not necessarily affect international transit traffic - for example, in January 2011 all access to foreign websites from Egypt was shut down on government orders, however, some international transit traffic appears to have been allowed.[35]

Interference for surveillance purposes

Internet traffic may be intercepted as it transits across third countries. As stated above, the traffic is not routinely stopped at borders and at a technical level it ignores their existence. However, there are places in the network infrastructure where interception is able to occur. Vulnerable points for traffic interception are at the so-called 'peering points' where different network providers connect to each other and exchange traffic. Interception at peering points occurs at the routing layer[36]. Additionally, Internet traffic can be intercepted after cable landing points, that is, the places where the physical cables carrying international traffic across the sea and overland connect to each other. For example, the British government's intelligence service, known as GCHQ, is alleged to have intercepted international Internet traffic for government surveillance purposes, under the code name of Project Tempora, which operated by monitoring traffic at cable landing points for trans-Atlantic traffic on British territory. The information on Project Tempora is not clear, but it has been reported that the British intelligence services were able to access content of email messages and recordings of phone calls, as well as web browsing histories.[37] This form of interception is surreptitious and unlike some of the other forms of interference discussed in this report, it would not be perceived by Internet users.

---

[32] Thou shalt not kill, in The Economist April 2013.

[33] Akdeniz p19.

[34] Akdeniz, p 19. Clause 3 of the "Order of the Azerbaijan Republic Ministry of Communications and Information Technologies" issued on 24 February 2000

[35] Source: Egypt Leaves the Internet by Jim Cowie, published on 27 January 2011, by Renesys.com. See http://www.renesys.com/2011/01/egypt-leaves-the-internet/

[36] See for example, German Internet Exchange Points as Targets for Surveillance, in Datacentres.com, 3 July 2013.

[37] GCHQ taps fibre-optic cables for secret access to world's communications, in The Guardian, 21 June 2013

Access to Internet traffic data, such as email and web surfing metadata, is another form of interference for surveillance purposes. A current example is the Prism programme operated by the United States' National Security Agency (NSA). Prism targeted access to communications traffic data of foreign nationals, held on the servers of companies operating content layer services. Those companies included the search engines Google and Yahoo, social media platform Facebook, voice services provider Skype, as well as Apple and Microsoft. The available information suggests that data obtained under the Prism programme included details of video, voice calls, images, chat, email and file transfers for people outside the US.[38] It is not exactly clear how the Prism programme operated, but it is understood that the legal basis for the programme is the *Foreign Intelligence Surveillance Act of 1978, known as* FISA. This Act provided for the collection of intelligence data on foreign States and their agents. Under FISA, data could be gathered in some circumstances without a court order, or under an order from a dedicated, secret court created under the Act, which has the power to oversee warrants for collection of such data. The targeting of foreign traffic implies a cross-border effect, bringing Prism within the scope of this report.

The NSA and GCHQ Internet surveillance programmes were exposed in June 2013 by the former US intelligence analyst Edward Snowden, however their exact mode of operation remains unclear at the time of writing. It is not confirmed, for example, if the collection of data is limited to communications traffic data or 'metadata', or if it extends to reading of content. Neither is it known if the persons performing the interception can identify individuals by name and locate them, or whether any intercepted content is ever blocked or if it is always allowed to transit onward. These questions would need to be addressed in order to establish the elements of a Recommendation on interception of international Internet traffic.

Interference for international travellers

There are new situations emerging where international travellers could be hit by different regimes of Internet restrictions on their access to content, services and applications. For example, users of cloud computing services may expect to get the same access to their content in any State or jurisdiction. If any form of blocking or filtering is implemented, they could find that they do not get the same access across all jurisdictions and that in some States, their access is interfered with. Similarly, mobile roaming users may experience different levels of access in different jurisdictions. The implications of this are, at the time of writing, not well understood and further research could be warranted.

Legal aspects of cross-border interference

The analysis of cross-border interference would seem to suggest that there is a common thread running between the different forms of interference, namely that the action occurs in one State that is 'upstream' but the effect is felt in another State that is 'downstream'. The effect appears to be the same whether the action is carried out by a State-owned network or a commercial network acting on behalf of the State, hence ownership of the network that is interfering does not appear to be relevant to the issue. Similarly, the effect may be the same if the interference is caused by error or be deliberate action. However, where the effect is caused by error, there is a greater likelihood that it can be resolved by technical co-operation. Hence, the problematic aspect is when the interference is caused by a deliberate action or policy on the part of the upstream State.

At the time of writing, there is no case law that deals with cross-border flow of Internet traffic and interference which may have an impact on access to content, services and applications. This means that an analysis of the legal position can only assess case law regarding elements of the problem and draw assumptions as to how a court may view the matter.

[38] The US confirms that it gathers online data overseas. In The New York Times, 6 June 2013; NSA Prism program taps in to user data of Apple, Google and others, in The Guardian, 7 June 2013.

In this section, the elements are divided as follows. The section begins with blocking and filtering policies, describing what they are and instances drawn from internal, domestic policy in Member States. Next we consider why blocking policy is an Article 10 matter, drawing on a limited volume of case law from the European Court of Human Rights and the European Court of Justice, and policy debates in the European Parliament. Thirdly, we consider how Article 10 applies regardless of frontiers, and fourthly we conclude with a discussion of how the obligations of Member States under the European Convention on Human Rights (ECHR) might be considered by a court.

It is further noted that the legal position surrounding interception of Internet services, as in the Tempora and Prism examples, is different from that of blocking and filtering. We will summarise the position as far as can be ascertained.

Blocking policies

Blocking or filtering may be instituted by means of the State prescribing measures by law to address certain types of content on a national basis, or by means of court orders to do so in respect of a specific complaint. In each case, the Internet service provider is told to block or filter certain content, and they may be informed of specific web addresses, URLs, IP addresses or domain names. There are also examples of the State seeking to encourage agreements between providers, which are not enshrined in law but could have a similar effect.

An example of a measure prescribed by law is Ley Sinde in Spain, which set up a system for orders to block websites that allegedly infringe copyright. In Britain, the State is seeking 'voluntary measures' to encourage an agreement between the Internet service providers whereby they would implement filters for default blocking of content deemed to be pornographic.

Blocking policies may also be implemented by means of notice and takedown measures. Notice and takedown is the term generally used where a notice is issued against particular content for its removal by either a hosting or platform provider, or by the Internet service provider. In the latter instance, it may be referred to as notice and action, a term coined by the European Commission, referring to actions other than removal of the content from the servers. Such action could be the blocking by the Internet Service Provider using equipment on another layer of the network. It could also refer to the blocking of payment facilities, as described above.

Notice and takedown may be enshrined in law, where it may be enforced by the State that has jurisdiction over the servers, for example, as proposed in 2013 by the European Commission[39] Alternatively, it may be implemented as a voluntary measure by the company operating the service. Notice and takedown may create cross-border effects since the jurisdiction in which the servers reside may be different from the jurisdiction that applies to the operator of the service or its users.

Notice and takedown is relevant in the context of social media, where small amounts of content are uploaded by individuals on a large scale, and may be subject to libel or defamation law, or law governing hate speech. The issues here are not yet well understood, and could warrant further study.

Where there are no other measures in place, blocking policies may be implemented by means of a court order. There are several examples of blocking being the subject of a court order to protect copyright, including the British cases related to Newzbin and The Pirate Bay. The founders of the latter took their case to the European Court of Human Rights. Although they were not successful and the Court agreed with the balance found by the national court[40], it did make some clarifications in its ruling that are relevant to the cross-border Internet context. Of particular interest, the court said that the Article 10 rights apply 'not only to the content, but also to the means of transmission or reception

[39] Directive on procedures for notifying and acting on illegal content hosted by online intermediary service providers (Directive on notice and action procedures)

[40] The court considered the balance between the Article 10 "right to freedom of expression" and the Article 1 "right to property" as it would apply to copyright.

since any restriction on the means necessarily interferes with the right to impart or receive'[41]. In other words, the Court confirmed that Article 10 rights apply to the network layer (see above).

However, blocking policies, whether court orders or government measures, become especially interesting in the Article 10 context when overblocking is found to occur. For example, a Yaroslavl court ordered Internet provider Netis Telekom to block access to a neo-Nazi blog hosted on the Live Journal social media platform and requested the ISP to block access to a certain IP address (208.93.0.128). This resulted in blocking access to the whole site[42].

In another example, in May 2008 a court in Ankara, Turkey, issued an order to block 10 allegedly illegal video files hosted on the video streaming site, YouTube. However, users found alternative ways around the block, and so, in June 2010, a supplementary blocking order was issued to block 44 additional IP addresses related to YouTube. Blocking all of these 44 IP addresses disrupted service to 10 other Google services that were not subject to any blocking order, and in some cases, it resulted in their services being totally unobtainable in Turkey. These services included Google Maps, Translate, and Notebook. In other words, as a result of one court order, 10 other services were also blacked out or disrupted[43].

Whilst these appear to be examples where the block was ordered with political interests in mind, another example from Britain illustrates how over-blocking can occur in a democratic society, where a block is ordered to protect commercial interests. In this example, a block ordered to protect football copyrights resulted in other sites, including the BBC's Radio Times, allegedly being unobtainable[44].

The blocking to prevent the downloading of material was considered by the European Court of Justice in the case of Scarlet Extended in 2011. The case concerned a national court ruling that required an Internet Service Provider to install a filtering system that would filter all communications with the aim of preventing the downloading of specified copyrighted material. The ruling stated that filtering systems could potentially undermine Article 10 rights, because such a system 'might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications' - in other words, it could lead to overblocking[45].

Why blocking policy is an Article 10 matter

Article 10 ECHR is a two-way right to impart and receive information without interference from a public authority. Government measures to block certain content on a national basis, or court orders to do so in respect of a specific complaint, may engage Article 10 in their own right. However, the complexity of the Internet and its layered structure (see above) raises other ways in which Article 10 may be engaged.

According to Professor Yaman Akdeniz, of Istanbul Bilgi University, [46] over-blocking may go well beyond the intentions of the State authorities and it would seem that a "*broadly-worded order would*

---

[41] European Court of Human Rights, Application no. 40397/12 *Fredrik NEIJ and Peter SUNDE KOLMISOPPI against Sweden*, p9.

[42] Account drawn from Akdeniz, p14.

[43] Ankara 1st Criminal Court of Peace, supplemental Decision no 2008/402 Misc, date 17.06.2010. This account is incorporated from Akdeniz, p13.

[44] *The Football Association Premier League Ltd v. BT and others*, Case No: HC13F02471 in the High Court of Justice, London. The alleged blocking of other sites was reported in The Register: Own Goal! Hundreds of websites blocked after UK Premier League drops ball, 15 August 2013.

[45] European Court of Justice, Case C70/10, 24 November 2011, *Scarlet Extended SA v. Société belge des auteurs*, compositeurs et éditeurs

[46] This account of the Article 10 interpretation is incorporated from Akdeniz, pp 11-12; & 15

be in breach of Article 10 and would be regarded as disproportionate, since the exceptions to Article 10 of the European Convention on Human Rights must be narrowly interpreted and the necessity for any restrictions must be convincingly established"[47]*.* In one important case, that of *Ahmet Yildirim v. Turkey*,[48] the matter of overblocking has been tested in the European Court of Human Rights. In *Yildirim v. Turkey*, a blocking order was specific to a piece of content hosted online, but over-broad in terms of the block that was ordered. It concerned a decision by a Turkish court "*to block access to Google Sites, which hosted an Internet site whose owner was facing criminal proceedings for insulting the memory of*" the founder of the Turkish State*, " Atatürk". As a result of the court decision, access to all other sites hosted by Google Sites was also blocked"*[49]. The applicant had hosted his websites on Google Sites. They were not the subject of the blocking order, but were nevertheless blocked as a result of its implementation.

Taking an Article 10 interpretation of this court order, "*the responsible public authority made it technically impossible to access any content on Google Sites in order to implement the measure ordered by the local court. The measure in question therefore amounted to interference by the public authorities with the applicant's right to freedom of expression. Such interference would breach Article 10 unless it was prescribed by law, pursued one or more legitimate aims and was necessary in a democratic society to achieve such aims.*"[50]

Furthermore, the European Court of Human Rights, "*finding a violation of Article 10 of the European Convention on Human Rights, held that a restriction on access to a source of information is only compatible with the Convention if a strict legal framework is in place regulating the scope of a ban and affording the guarantee of judicial review to prevent possible abuses*[51]*"*. The exceptions to Article 10 should be narrowly interpreted and the necessity for them should be convincingly established.

In *Yildirim v. Turkey*, "*the Court further observed that there was no indication that the Criminal Court had made any attempt to weigh up the various interests at stake, in particular by assessing whether it had been necessary to block all access to Google Sites. In the Court's view, this shortcoming was a consequence of the domestic law, which did not lay down any obligation for the courts to examine whether the wholesale blocking of Google Sites was justified. The courts should have had regard to the fact that such a measure would render large amounts of information inaccessible, thus directly affecting the rights of Internet users and having a significant collateral effect*"[52].

Therefore, even provided that a legal basis exists for blocking access to websites, any interference must be proportionate to the legitimate objective pursued. Within this context, following Yildirim v. Turkey, blocking access to web portals and social media platforms is arguably a serious infringement on freedom of expression and *incompatible with Article 10 of the European Convention*

[47] Akdeniz, p15

[48] *Ahmet Yildirim v. Turkey*: Application No. 3111/10, Judgment of 18 December 2012, 18.03.2013 (final).

[49] Press release issued by the Registrar of the court, ECHR 458 (2012) Restriction of Internet access without a strict legal framework regulating the scope of the ban and affording the guarantee of judicial review to prevent possible abuses amounts to a violation of freedom of expression. In the case of Ahmet Yildirim v. Turkey: Application No. 3111/10, Judgment of 18 December 2012, 18.03.2013 (final).

[50] Akdeniz, p11

[51] Akdeniz p12

[52] Press release issued by the Registrar of the court, ECHR 458 (2012) Restriction of Internet access without a strict legal framework regulating the scope of the ban and affording the guarantee of judicial review to prevent possible abuses amounts to a violation of freedom of expression. In the case of Ahmet Yildirim v. Turkey: Application No. 3111/10, Judgment of 18 December 2012, 18.03.2013 (final).

on Human Rights, and potentially *would be more far reaching than is reasonably necessary in a democratic society*[53].

Article 10 applies regardless of frontiers

Blocking policy is usually regarded as a domestic, national matter for States to determine for themselves. However, in the context of cross-border Internet traffic, that situation may be altered. There is no existing case law, but an extrapolation of certain cases of blocking into the cross-border situation does suggest that there is a new issue arising concerning jurisdiction over content policy.

In the case of *Yildirim v Turkey*, the European Court made a statement that may be relevant to any future cross-border cases. The European Court stated that "*Article 10 applied not only to the content of information but also to the means of disseminating it*"[54] and reminded us that under Article 10(1) of the Convention, the right to freedom of expression applies "*regardless of frontiers*".

In this section, we will examine as far as possible what that could mean. The legal question is whether the Contracting States of the Council of Europe would be responsible for breaches of the European Convention on Human Rights if their state level blocking or filtering policies have cross border implications in another neighbouring state.

"Taking a hypothetical case, the question would be whether an applicant based in State B can complain of acts (in this scenario blocking access to websites) which can be attributed to State A even though the acts were not performed on the territory of State B[55]*. In such a scenario the European Court would assess the connection between the applicant from State B and the respondent State A and whether the impugned act (access blocking) had effects outside the territory of State A (the extra-territorial act)"*[56].

Professor Yaman Akdeniz explains that this raises a complex legal argument concerning jurisdiction. *Article 1 of the European Convention on Human Rights states that: 'The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of [the] Convention." It follows from Article 1 that Member States must answer for any infringement of the rights and freedoms protected by the Convention committed against individuals placed under their "jurisdiction'. Accordingly, 'the exercise of jurisdiction is a necessary condition for a Contracting State to be able to be held responsible for acts or omissions imputable to it which give rise to an allegation of the infringement of rights and freedoms set forth in the Convention.' Therefore, a Contracting Party 'is responsible under Article 1 of the Convention for all acts and omissions of its organs regardless of whether the act or omission in question was a consequence of domestic law or of the necessity to comply with international legal obligations.' Furthermore, Article 1 makes no distinction as to the type of rule or measure concerned and does not exclude any part of a Contracting Party's "jurisdiction" from scrutiny under the Convention*[57]*.'*

U*nder international law, a State's jurisdiction is primarily territorial*[58]*,* but is not necessarily restricted to it[59]. *The European Court of Human Rights has accepted that in exceptional circumstances*

---

[53] This account of the Article 10 interpretation is incorporated from Akdeniz, pp 11-12

[54] Akdeniz, p19

[55] Akdeniz, p18

[56] This legal argument is incorporated from Akdeniz, pp16-18.

[57] Akdeniz, p16

[58] Akdeniz, p17

[59] Under international law, there are complementary principles of jurisdiction: personal (passive and active), effective, preventive and universal. Source: Joanna Kulesza. There is also an emerging notion of 'extra-territorial extension of sovereignty' where territorial jurisdiction is applied to online platforms that operate across State borders. Source: Paul Fehlingher.

the acts of Contracting States performed outside their territory, or which produce effects there (extraterritorial acts), may amount to exercise by them of their jurisdiction within the meaning of Article 1 of the Convention. The European Court has recognised a number of exceptional circumstances capable of giving rise to the exercise of jurisdiction by a Contracting State outside its own territorial boundaries: "in each case, the question whether exceptional circumstances exist which require and justify a finding by the Court that the State was exercising jurisdiction extra-territorially must be determined with reference to the particular facts."[60] *"Furthermore, in Al Skeini and Others v. The United Kingdom, the European Court held that that it does not mean that 'jurisdiction under Article 1 of the Convention can never exist outside the territory covered by the Council of Europe Member States.' "*[61]

"Hence, it could be argued that in exceptional circumstances, States could be held responsible for actions taking place outside their territorial jurisdiction. In the hypothetical scenario outlined above, blocking of Internet content could be considered as such as exceptional case, even though the impugned act takes place outside its territorial jurisdiction". [62]

Obligations of Member States under ECHR Article 10

A position is therefore shaping up that States can be held responsible for Internet access blocking that takes place in another State.

"The next legal question concerns "who controls the conduct that harms the rights as defined in the ECHR." Al Skeini and Others v. The United Kingdom stated that 'jurisdiction means no less and no more than authority over and control of' and that 'jurisdiction is neither territorial nor extra-territorial: it ought to be functional' in relation to Convention rights.

In our hypothetical scenario, the state implementing the blocking policy would be in control, with detrimental cross border impact of that policy in a neighbouring state. The European Court has held that although the essential object of many provisions of the Convention is to protect the individual against arbitrary interference by public authorities, there may in addition be positive obligations inherent in effect respect of the rights concerned, in this case under Article 10.

The European Court emphasized the key importance of freedom of expression as one of the preconditions for a functioning democracy in a number of its decisions and it has established that genuine, effective exercise of this freedom does not depend merely on the State's duty not to interfere: it may require positive measures of protection"[63.]

According to Professor Yaman Akdeniz, in determining whether or not such a positive obligation exists, regard must be had to the fair balance "*that has to be struck between the general interest of the community and the interests of the individual, the search for which is inherent throughout the Convention. The scope of this obligation will inevitably vary, having regard to the diversity of situations obtaining in Contracting States and the choices which must be made in terms of priorities and*

---

[60] This argumentation is incorporated from Akdeniz, p18. See *Loizidou v. Turkey*: judgement of 18 December 1996, Reports of Judgments and Decisions 1996-VI, pp. 2235-2236 § . See among others *Drozd and Janousek v. France and Spain*, judgment of 26 June 1992, Series A no. 240, § 91; *Loizidou v. Turkey* (preliminary objections), 23 March 1995, § 62, Series A no. 310; *Loizidou v. Turkey* (merits), 18 December 1996, § 52 :Reports of Judgments and Decisions 1996 VI. The statement of principle, as it appears in Drozd and Janousek and the other cases is very broad: the Court states merely that the Contracting Party's responsibility "can be involved" in these circumstances (*Al Skeini and Others v. The United Kingdom*, Application no. 55721/07, 7 July 2011, para 133). Note also *Mohammed Ben El Mahi and Others v. Denmark* (App. No. 5853/06), 11 December 2006 (admissibility decision). See also *All Skeini and Others v. The United Kingdom*, Application no. 55721/07, 7 July 2011, para 132

[61] Akdeniz, p18

[62] Akdeniz, p18

[63] This legal analysis is incorporated from Akdeniz, pp20-21.

resources. Nor must such an obligation be interpreted in such a way as to impose an impossible or disproportionate burden on the authorities.

Based on the positive obligation to protect principle developed by the European Court, it can be argued that Contracting States do have a positive obligation to ensure that they do not interfere with the cross border flow of the Internet from their territories to neighbouring states. If a particular Contracting State or an Internet Service Provider based in that Contracting State provides Internet access to a neighbouring state, then the Contracting State is obliged to ensure that restrictions that may be imposed locally should not interfere with the free flow of information and Internet access within the neighbouring state(s).

As established in Yildirim v. Turkey, blocking access to a website would constitute interference with the exercise of the rights guaranteed by Article 10(1) of the European Convention as Article 10 applies not only to the content of the information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information."

Professor Yaman Akdeniz states that "*it is arguable that if a Contracting State - within its authority - controls the conduct that harms the rights and freedoms defined in the European Convention in a neighbouring state by interfering with that state's Internet access, traffic, or access to information then state liability for those harms should arise."*[64]

Moreover, there is some case law to suggest that the liability of a Member State is not limited to what happens within its own territory and that in some circumstances, it may be liable for matters occurring in another State where its own citizens are incurring a harm[65].

Legal aspects: interception for State surveillance purposes

Interception of traffic, either at the cable landing points or peering points, is government by a different legal framework from blocking and filtering of content. In terms of Convention rights, it primarily engages Article 8, the right to privacy as a necessary protection of the Article 10 rights. From what can be ascertained at the time of writing, the two projects Prism and Tempora have been established under an agreement made in 1946 between the British and United States military, and later known as the UKUS Agreement. [66] In general, interception of communications traffic is governed by laws that cover surveillance and the intelligence services, and will usually fall under a justice ministry portfolio; whereas blocking and filtering is typically addressed under telecommunications law regulating the commercial activities of network providers, and will usually fall under an industry or media ministry portfolio.

Challenges regarding cross-border interference

The key challenges in this context concern the rights and responsibilities of Member States with regard to the content policies of other States. In particular, the challenge is to establish whether there is a duty or responsibility on Member States to protect the rights of their citizens where they are

[64] This argument is supported by Council of Europe: Proposals for international and multi-stakeholder co-operation on cross-border Internet: t Interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services, p16, pt.60 . This point refers to the International Law Commission's work on State liability: ILC Draft articles on Prevention of Transboundary Harm from Hazardous Activities (2001) (Yearbook of the International Law Commission, 2001, vol. II, Part Two) p. 150

[65] *Ilascu and others v Moldova and Russia*, Application no. 48787/99, Judgement 8 July 2004

[66] It was signed as the British-US Communication Intelligence Agreement in 1946, and from 1956 became known as the UKUSA Agreement. Available at: http://filestore.nationalarchives.gov.uk/ukusa/hw-80-4.pdf

infringed by the policy of another State, and what form that could take. In that regard, the challenge extends to how Member States could protect their own jurisdiction over content policy.

States may consider taking direct and specific action to block access to content. They may also implement a general policy towards content that requires certain categories of content to be blocked. Even a well-targeted policy can have unintended consequences such as overblocking or blocking in error. In either case, if Internet services are being supplied across borders, then the blocking policy is likely to affect the second State and the question must arise as to the possibility for incursions into State sovereignty in those instances.

The implications are that people will be subjected to social policies and political sensitivities and censorship of foreign states. A speech, whether commercial or political, with an international dimension will be curtailed with a range of possible political and economic consequences. The following scenarios are hypothetical but they serve to illustrate more tangibly the situations that could arise.

Upstream blocking or filtering policies adopted by States or commercial actors

"State A adopts a policy of blocking, using either the routing layer (DNS and/or IP based blocking) or application layer. An Internet Service Provider (which may be State owned or private) based in State A provides Internet access in another neighbouring state (State B). The ISP maintains the blocking policy of State A in the services offered in State B.

Assuming that the neighbouring State B has no control over the services offered by the ISP, and is unable to get the ISP to remove the blocking policy for its citizens, then this may lead to unintended consequences in State B. For example, if the blocked content is legal in State B, then the Convention rights of citizens in State B to receive information are being infringed. Their rights to impart information would also be infringed, since they would have to comply with the blocking policy of State A, even though they would not reside within its jurisdiction.

In essence, State B would have lost the ability to manage its own communications policy in regard to content and its sovereignty with regard to communications policy risks being eroded"[67].

According to Professor Yaman Akdeniz *"The important question that would arise in this scenario is whether the Contracting States of the Council of Europe would be responsible for breaches of the European Convention on Human Rights if their state level blocking or filtering policies have cross border implications in another neighbouring state. In a hypothetical case the question would be whether an applicant based in State B can complain of acts (in this scenario blocking access to websites) which can be attributed to State A even though the acts were not performed on the territory of State B"*[68].

In such a scenario, the European Court would assess the connection between the applicant from State B and the respondent State A and whether the impugned act (access blocking) had effects outside the territory of State A (see above, Legal Aspects).[69]

Blocking order by a court results in overblocking, affecting speech in another State

A court in State A orders content on a social website to be blocked for political reasons. The court is specific as to the content that is to be blocked. It asks for the block to be implemented in the routing layer, and provides a list of IP addresses. When the Internet service provider implements the block, it is discovered that content which is not subject to the court order is also blocked – in other

[67] Example paraphrased from Akdeniz, pp15-16

[68] Akdeniz, p16

[69] Akdeniz, p18

words, over-blocking has occurred. Among that over-blocked content is a website owned and run by a citizen of State B, who is entirely innocent and unconnected with the reasons for the blocking order. His website has been rendered invisible and he is prevented from carrying on his lawful trade or profession, or from disseminating legitimate political speech in State B. The issue is what redress that citizens should have in terms of their Article 10 rights.

Altering or blocking using the DNS system following law enforcement request

Law enforcement authorities in State A approach a domain registry and request that it removes a particular domain, owned by someone in State B, from its register. The registry complies, and all websites hosted on that domain will disappear from the Internet and will no longer be able to be accessed. That block on access will be experience by anyone, from any State, and regardless of whether or not the website content is legal in countries outside of State A. Moreover, if legitimate content that is not the subject of the block is also hosted on that domain, it too will disappear from the Internet.

State B may have jurisdiction over the websites if they reside on servers that are physically located within its territory, but it will have no jurisdiction over the Registry which in State A. Under international law, it may be that State B could have a duty to do what it can to protect the Article 10 rights of its citizens. The issue is what redress can be available for citizens of State B terms of their Article 10 rights.

An international multi-blocking scenario

The concern here is the rights of speakers who wish to transmit their message across borders, and have a reasonable expectation that their message will be transmitted and accessed, without them having to know where the readers are.

Under this scenario, there is a multitude of blocking policies in place among the various member states who have signed the Convention. We assume either that the blocking policies have been imposed by law and that they address social policy goals; or that they have been implemented by commercial actors to serve their own business purposes. We also assume that the policy criteria for blocking vary across the different member states.

An individual in State A wishes to impart information via their own website. However, he discovers that the blocking policies in some other member states are resulting in his website being blocked. He is unable to identify whether this is the case in all states, and to what extent the blocking policies are restricting access to his site.

This scenario is intended to illustrate how the rights of the speaker to express legal views may be curtailed if blocking policies become widely implemented. The speaker could be any individual, whether private person, politician, business or professional who has a message with an international dimension. Speakers cannot know how blocks and filters will be implemented by the many different ISPs that serve all of the Member States of the Convention. However, if their speech is blocked, whether or not the block is intentional, then their right under Article 10 must be engaged.

The legal position here is complex. If his content is deemed to be illegal in the receiving state (State B), then no obligation arises. However, if his website is legal and not breaking the law in State B, and his content is being restricted in violation of Article 10 ECHR, then a positive obligation may arise. In this situation the duty of due diligence may be relevant:

"The commitment of a state in respect of taking measures to prevent, manage and respond to transboundary disruptions or interferences would be one of due diligence. It is the conduct of the state in question that would determine whether it has complied with its duty of due diligence. (.) Acting with

due care imposes on a state a duty to do all it can, or in other words, to take all appropriate measures at its disposal to prevent and minimise foreseeable significant transboundary harm."[70]

RECOMMENDATIONS

1. New Instrument regarding Internet traffic and interference which may have an impact on access to content, services and applications:

   a/ Liability for harms resulting from interference with access to Internet content: If a Contracting State "within its authority" controls the conduct that harms the rights and freedoms defined in the European Convention in a neighbouring state by interfering with that state's Internet access, traffic, or access to information then state liability should arise.

   b/ Sovereignty of States in respect of interference with access to content: Unless a Member State agrees that certain content should be blocked, it should have the right to have that content available within its jurisdiction. Applying another State's blocking policy infringes on its sovereignty. The position is especially grave where overblocking can be shown to be occurring, and where the measure is also filtering out content uploaded by citizens of the affected State.

   c/ Due diligence duty in respect of blocking of content in another State: if a State controls the conduct that harms the rights, that is, the conduct of the filtering ISP, then that State might be under international liability for infraction of free speech.

2. Possibility of incorporating or drafting a new instrument regarding interception of communications and surveillance. It is recommended that a separate Instrument be developed for interception of cross-border Internet traffic, in the context of the recently revealed surveillance projects.

   a/ These forms of interception are government by a different legal framework from blocking and filtering of content.

   b/ there remain many question marks around the functioning of unaccountable government's Internet surveillance and further research could be valuable in establishing the form and elements of a new CoE Instrument

3. Other areas for further study

   The matter of cross-border Internet in an Article 10 context is complex. Three possible areas for further study have been identified in this report.

   a/ How to address DDOS or other form of cyber-attack that has a political motive; in particular, whether it could be construed as 'speech'.

   b/ International services at the application and content layer, especially services for international travellers such as mobile data roaming, and cloud computing services - in these specific contexts, the rights and responsibilities of Member States are unclear, with regard to restrictions on content being applied to their citizens who are travelling across borders.

[70] Council of Europe Proposals for international and multi-stakeholder co-operation on cross-border Internet: Interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services, p17-18, pt72.

c/ Web platforms, notably social media and user-generated content: the legal and human rights issues in these contexts are complex and currently not well understood.

APPENDIX I

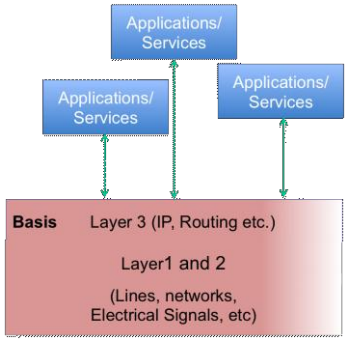
Cross-border flow of Internet traffic and interference which may have an impact on access to content, services and applications: Incidents affecting the cross-border flow of Internet traffic
Report by Professor Michael Rotert

The Internet model

The current design of the Internet is a network consisting of non-technically expressed two layers - the infrastructure layer (Basis) with all the network equipment like routers, switches, lines etc. and the application layer with innumerable programs.

A development goal of the Internet architecture was to have applications connected to the net no matter on which infrastructure or operating system. There were also standard applications defined like e-mail, file transfer etc. Another goal was to be able to communicate no matter between humans or between machines or between machines and humans by means of these applications without taking care of the nature of the physical infrastructure or transport system. In the beginning it started with slow fixed lines and local area network cabling. But no matter if broadband fixed lines or radio communication, leased lines, transatlantic lines or dialup lines, point-to-point lines or satellite links, it should work without knowing about the infrastructure. All these different connection types may exist in parallel, media independent.

Cross border flow of Internet traffic can therefore be looked at on several layers. In order to formalize the way of tackling the problem the areas where these problems are occurring have to be defined.



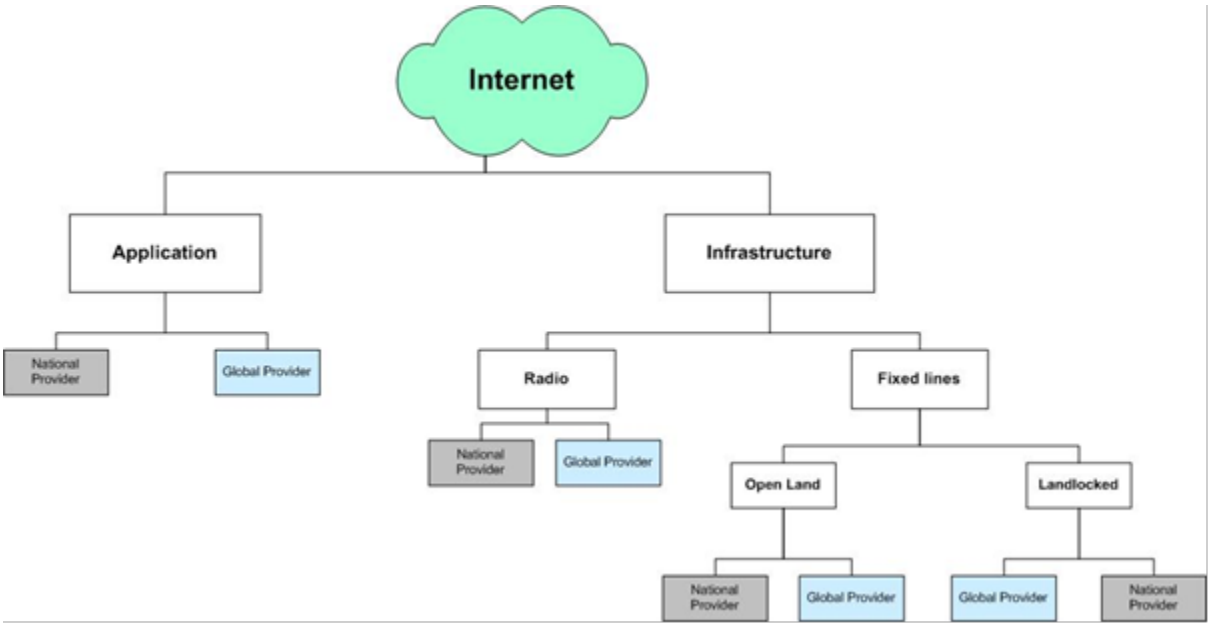
For further simplification certain assumptions have to be made:

Incidents should be major only if a significant part of the population is affected or if an industry for basic services (power, water etc.) or basic services themselves are affected. This does not mean that others are not as important it is only for simplification. Nevertheless below are major incidents listed which may not fit into that scheme.

In many parts of the world there is a tendency for network peering points in order to have short and therefore cheaper lines/bandwidth to connect to the Internet. Of course these peering points are under the jurisdiction of the country where they are located. So sometimes it may not be feasible to connect to them; it depends on the relation between the countries and the area the peering point is located.

There is also a tendency of China to supply small nations in the neighbourhood with subsidised and therefore cheap and affordable internet connections. These connections may be filtered and intercepted according to Chinese jurisdiction. International law should take care of those cases. Also connections to the US maybe intercepted at any time according to US law without further notice to the connected country. This should always be clearly made public and stated within the contract between the parties! Any influence on the basis of those connections is hard to find and it is even harder to solve problems having these kind of configurations.

In order to look at threats within an environment different to the above situations it might be useful to illustrate the overall situation in a graph as follows:



As threats on the application layer we will find

- DDoS attacks (denial of service attacks)
  Single individuals, a group of hackers or criminals or even (foreign) authorities can execute DDoS attacks.

  Targets can be businesses, government web sites, e-government applications or even name servers which in turn may affect the whole country.

  Either access providers within the country or the affected institution itself can react in order to prevent outages. Also the global access provider can even take measures before the attack reaches the border or the destination network. The provider gets the knowledge of such an attack by recognizing the amount of traffic, forecast systems are possible but subject to deep packet inspection.

  In case of an affected national name server, additional secondary servers which should be in place sometimes even in a neighbour or affiliated country can replace the function of the primary name server. There are no technical differences to ask the primary server first. The authoritative server who answers first is the one who is chosen. So backups outside the country could be a remedy. There are more threads if for whatever reasons all nameservers of a domain are located outside the country. This situation should be avoided in any case.

  A very special incident with nameservers was the case of Wikileaks (see below). These kinds of effective blocking by modifying the entry within the database of the Top Level Domain can only happen if governments and providers are cooperating and the services are all within the same jurisdiction or at least all parties are willing to cooperate strongly. Threats in this area should be subject to international treaties. Therefore Top Level Domains of common use and interest should be located within a neutral environment or only to follow international law.

- Any other malware on the application level can be dealt with local security.

Attackers try to overtake local sites of critical infrastructure like power plants, water supply companies etc. An example happened some time ago with STUXnet where systems where effected even if not directly connected to the Internet. It should be known meanwhile what to do, how to take care of such a problem. I doubt it, that this is done already in all necessary places. Awareness raising should go on. This is a national issue.

Remedies are depending very much of the systems, their software and are in general securing the system. In a number of cases it might be necessary to replace the system in order to obtain latest software versions. National or international experts can accomplish this.

Blocking on the infrastructure as remedy to problems in the application layer is dangerous. It may cause collateral damages (overblocking) or even disturb heavily the normal network operation outside the blocking area even other parts of the Internet!

Threats on the Infrastructure layer

This layer needs more aspects to look at as can be seen on the graph above.

Lines can be cut off before crossing the border or foreign radio stations may jam the frequency band used for Internet connections. The latter works at least in the border area.

The footprint of a satellite can hardly be affected as long as the satellite operator and the provider feeding a jam stream are cooperating. Satellite dishes for two way communication are not very common due to price and bandwidth, but this medium could even be used if the national government tries to cut people off of the Internet.

If all Internet connections coming into a country via radio signals from abroad, international treaties have to be in place in order to secure the connection. Again, backup systems are a remedy as protocols are in place to switch automatically to other connections in case of outages.

In case of lines the problems and remedies are similar to the radio connections however it is normally easier to control lines.

Land-locked countries may be in an even worse situation but this is currently addressed by the ITU, a grouping within the UN:

RESOLUTION PLEN/1 (DUBAI, 2012)

Special measures for landlocked developing countries and small island developing states for access to international optical fibre networks

The World Conference on International Telecommunications (Dubai, 2012),

considering

a) Resolution 65/172 of 20 December 2010 of the United Nations General Assembly, on specific actions related to the particular needs and problems of landlocked developing countries (LLDCs);

b) Resolution 30 (Rev. Guadalajara, 2010) of the Plenipotentiary Conference, on special measures for the least developed countries (LDCs), small island developing states (SIDS), LLDCs and countries with economies in transition;

c) the Millennium Declaration and the 2005 World Summit Outcome;

d) the outcome of the Geneva (2003) and Tunis (2005) phases of the World Summit on the Information Society (WSIS);

e) the Almaty Declaration and Almaty Programme of Action addressing the special needs of LLDCs within a new global framework for transit transport cooperation for landlocked and transit developing countries,

recalling

a) the New Partnership for Africa's Development (NEPAD), which is an initiative intended to boost economic cooperation and development at regional level, given that many landlocked and transit developing countries are in Africa;

b) the Declarations of the ministers of communications of the Union of South American Nations (UNASUR) and the Roadmap for South American connectivity for integration of the Telecommunications Working Group of the South American Infrastructure and Planning Council (COSIPLAN);

c) Mandate No. 7 arising from the sixth Summit of the Americas, held in Cartagena, Colombia, on 14-15 April, 2012, in which the Heads of State and Government of the Americas resolved *"To foster increased connection of telecommunication networks in general, including fibre-optic and broadband, among the region's countries, as well as international connections, to improve connectivity, increase the dynamism of communications between the nations of the Americas, as well as reduce international data transmission costs, and, thus, promote access, connectivity, and convergent services to all social sectors in the Americas"*,

reaffirming

a) the right of access of landlocked countries to the sea and freedom of transit through the territory of transit countries by all means of transport, in accordance with applicable rules of international law;

b) that transit countries, in the exercise of their full sovereignty over their territory, have the right to take all measures necessary to ensure that the rights and facilities provided for landlocked countries in no way infringe upon their legitimate interests,

recognizing

a) the importance of telecommunications and new information and communication technologies (ICT) to the development of LLDCs and SIDS;

b) that current difficulties of LLDCs and SIDS continue to adversely affect their development,

4. *noting* that access to international optical fibre networks for LLDCs and the laying of optical fibre across transit countries are not specified in the infrastructure development and maintenance priorities in the Almaty Programme of Action,

conscious

a) that fibre-optic cable is a profitable telecommunication transport medium;

b) that access by LLDCs and SIDS to international fibre-optic networks will promote their integral development and the potential for them to create their own information society;

c) that the planning and laying of international optical fibre call for close cooperation between LLDCs and transit countries;

d) that, for the basic investment in laying fibre-optic cable, capital investments are required,

resolves to instruct the Director of the Telecommunication Development Bureau

1 to study the special situation of telecommunication/ICT services in LLDCs and SIDS, taking into account the importance of access to international fibre-optic networks at reasonable cost;

2 to report to the ITU Council on measures taken with respect to the assistance provided to LLDCs and SIDS under *resolves to instruct* 1 above;

3 to assist LLDCs and SIDS to develop their required plans containing practical guidelines and criteria to govern and promote sustainable regional, subregional, multilateral and bilateral projects affording them greater access to international fibre-optic networks,

instructs the Secretary-General to bring this resolution to the attention of the Secretary-General of the United Nations, with a view to bringing it to the attention of the United Nations High Representative for LDCs, LLDCs and SIDS,

invites the Council to take appropriate measures to ensure that ITU continues to collaborate actively in the development of telecommunication/ICT services in LLDCs and SIDS,

invites Member States

1 to cooperate with LLDCs and SIDS in promoting regional, subregional, multilateral and bilateral projects and programmes for telecommunication infrastructure integration that afford LLDCs and SIDS greater access to international fibre-optic networks;

2 to assist LLDCs and SIDS and transit countries in executing telecommunication infrastructure integration projects and programmes,

encourages landlocked developing countries and small island developing states to continue to accord high priority to telecommunication/ICT activities, by putting in place technical cooperation activities in order to promote integral socioeconomic development,

invites Member States, Sector Members, Associates and Academia to continue to support ITU Telecommunication Development Sector studies of the situation of telecommunication/ICT services in LDCs, LLDCs, SIDS and countries with economies in transition so identified by the United Nations and requiring special measures for telecommunication/ICT development.

For the land-locked problem similar solutions can be found for the Internet as for oil and gas cross border:

A number of problems arise from cross-border oil and gas transportation via pipeline. These problems, which are more acute in the case of pipelines passing through a transit country, fall into three broad categories: reconciling the interests of the different parties involved, the lack of an overarching legal regime to regulate activities, and rent-sharing among the parties (ESMAP, 2003). Specifically, transit oil and gas pipelines face potential disruption by the transit country. Recent developments in the gas dispute between Russia and Ukraine demonstrate the role of transit pipelines in the security of energy supply, as well as the importance of a sufficient understanding of fundamental transit pipeline economics.

Present and future pipelines face the risk of continuous conflict over legal, economic, and political issues.

Once the pipeline has been built and put into operation, the risk arises of disruption of the pipeline by the transit country over disputed transit terms. This is due to two key factors: first,

bargaining power shifts in favour of the transit country upon construction and operation of the pipeline; second, price changes that result from changes in the value of the throughput can affect the behaviour of the transit country. This is defined as the obsolescing bargain – a term coined by Raymond Vernon (1971). In the literature, the obsolescing bargain is a situation in which bargaining power shifts from a multinational company (MNC) to a host country government after investments have been made in a project and the project has started operations (Vernon, 1971). The concept explains the relations between the MNC and the host country.

These attacking methods and measures all apply to a full cut from communication by physical disruption of lines and signals.

But what happens if the cut is done within the protocol level (infrastructure layer)? Rerouting of data packets, routes taken off of the routing devices from neighbour ISPs or internationally acting ISPs are requested to delete routes to a whole country or specific areas or institutions those are threats which may look as malfunction of the network on a first glance. If a government or a kind of secret service gave the order for rerouting or deleting routes it should be covered under international law. If it was accidentally by configuration failure or malfunctioning devices. it is a technical issue which might be addressed in severe cases to the international Internet community.

Summary of Internet incidents with cross border effect

1. Affecting companies only

1.1 DDoS attacks cripple web heavyweights

2000

A series of DDoS attacks crippled or disabled large websites like Yahoo, CNN, Amazon, eBay, Buy.com, ZDNet, and online trading sites like E*Trade and Datek. The attacks were spread out over days and attacked different sites, but were thought to be connected. To name an example of the extent of the DDoS attack, Buy.com was hit with eight times more traffic than its maximum capacity.

1.2 The Code Red worm attacks web servers

2001

Code Red was a computer worm that spread itself via a security hole in the Microsoft IIS web server, even though a security patch had been out for months. The infected websites were defaced by the worm, showing the following message: HELLO! Welcome to http://www.worm.com! Hacked By Chinese!

1.3 The SQL Slammer worm wreaks Internet havoc

2003

SQL Slammer was a computer worm that spread itself rapidly via a security hole in Microsoft SQL Server. A security patch had been available for six months, but many had not installed it. At least 22,000 systems were infected, possibly many more

1.4 Big sites go dark as San Francisco datacenter loses power

2007

When 365 Main's datacenter in San Francisco lost power it effectively took down a number of big websites and services like Craigslist, Typepad, LiveJournal, Yelp, Second Life, Technorati and Adbrite. All of them were hosted at this supposedly super-reliable co-location facility. The incident was

made worse because several of the backup power generators failed to start. Although power was restored after about 45 minutes, it took hours before all the websites were back up and running.

1.5 RSA

2007

RSA is well known for two things: the amazingly useful public key encryption algorithm (which gave the company its name), and the RSA SecurID brand of hardware tokens for user authentication (which do not actually use the RSA algorithm). Today RSA is a subsidiary of EMC Corporation. In March, the company disclosed that it had been the target of a successful cyberattack in which the attackers obtained some type of information which allowed them to reduce the protection provided by the tokens. Within a few weeks it was reported that this information had been used in intrusion attempts at U.S. defense contractors, but there is little to suggest that the abuse is more widespread. Many customers were disappointed in RSA's reticence to share information about the attack, which would enable customers to make informed estimates of their own risk. Some were surprised that RSA would retain SecurID "key seed" data at all. (Ironically, the RSA algorithm is often used specifically to avoid sharing such secret keys unnecessarily.) We are dependent on our vendors.

1.6 SPAMHouse

2013

For instance the London peering point LINX was affected when the DDoS attack against SPAMHouse hit the UK. Other peering points noticed the enormous amount of traffic but there were no reason for those to counteract. Peering points would be an ideal point for implementing an early warning system. This would make it necessary to implement deep packet inspection to a certain extent (looking at every 100.000 packet would be enough for statistical software). According to data protection rules and customer protection it would be necessary to make measures mandatory by local law.

2. Affecting countries

2.1 Turkish ISP hijacks the Internet

2004

A Turkish ISP (TT Net) made a mistake when configuring its routers, effectively announcing to the rest of the Internet that everything should be routed to them. Routers talk to each other and propagate this kind of information, so the configuration error spread and resulted in tens of thousands of networks on the Internet sending traffic to the wrong destination or not getting the traffic they were supposed to.

2.2 Earthquake breaks Asian Internet

2006

A massive earthquake with an epicentre outside the coast of Taiwan broke a large number of important submarine communications cables. Internet traffic to and from China, Taiwan, Hong Kong, the Philippines, Malaysia, Singapore and many other places was severely affected by the incident, especially to the US.

2.3 The Mediterranean submarine cable break

2008

This was actually three separate incidents, but they happened so closely together that the effect was enormous (and launched a number of conspiracy theories). Between January 23 and February 4, 2008, a total of five submarine data communications cables in the Mediterranean outside Egypt were cut. These cables were part of the Internet backbone and the disruption severely limited the Internet access to and from the Middle East and India. Theories as to why the various cable breaks happened include damage done by ship anchors and bad weather conditions, although due to various circumstances there are some conspiracy theories about sabotage which have not been completely ruled out even by the UN (ITU).

2.4 China reroutes the Internet

2010

In April, China Telecom spread incorrect traffic routes to the rest of the Internet. In this specific case it meant that during 18 minutes, potentially as much as 15% of the traffic on the Internet was sent via China because routers believed it was the most effective route to take.

Similar incidents have happened before, for example when YouTube was hijacked globally by a small Pakistani ISP two years ago. Normally this results in a crash since the ISP can't handle the traffic. However, China Telecom was able to handle the traffic, so most people never noticed this. At most they noticed increased latency as traffic to the affected networks took a very long and awkward route across the Internet (via China).

Even though no serious outage happened as a result of this, we think it's such a fascinating disruption of the traffic flow that we felt it was worth including here. This is an inherent weakness of today's Internet infrastructure, which largely relies on the honour system. Renesys has a more in-depth explanation of this incident and how it could happen. We should state that it wasn't necessarily an intentional hijacking.

3. Affecting information only

3.1 The Wikileaks drama

2010

If you've missed this you must have been hiding under a rock, which in turn was buried below a mountain of rocks. The site issues that Wikileaks experienced during the so-called Cablegate were significant. First the site was the victim of a large-scale distributed denial-of-service attack which forced Wikileaks to switch to a different web host. After Wikileaks moved to Amazon EC2 to better handle the increased traffic, Amazon soon shut them down. In addition to this, several countries blocked access to the Wikileaks site. And then the possibly largest blow came when the DNS provider for the official Wikileaks.org domain, EveryDNS, shut down the domain itself. Without a working domain name in place, Wikileaks could for a time only be reached by its IP address. Since then, Wikileaks has spread itself out, mirroring the content over hundreds of sites and different domain names, including a new main site at Wikileaks.ch. As if this wasn't enough drama, you have to add the reactions from some of Wikileaks' supporters (not from Wikileaks itself). The services that cut off Wikileaks in various ways (Paypal, VISA, Mastercard, Amazon, EveryDNS, etc.) were subjected to distributed denial-of-service attacks from upset supporters across the world, which resulted in even more downtime. There was also collateral damage, when some attackers mistook the DNS provider EasyDNS for EveryDNS, aiming their attacks at the wrong target. **The Wikileaks drama is without a doubt the Internet incident of the year.**

3.2 Tehran Bob

2010

In March we learned that the Comodo Certificate Authority had been compromised via one of its small regional resellers and tricked into issuing fraudulent certificates for a variety of high-profile websites such as Google. An independent Iranian hacker claimed responsibility. In August, an alert user detected that fraudulent certificates were being used in a massive man-in-the-middle attack conducted against Gmail users in Iran. He found that Google's Chrome browser was giving warnings about the certificate appearing on Google's own websites. Word spread quickly that the Dutch CA DigiNotar had, in fact, been compromised for quite some time. In September DigiNotar earned the dubious distinction of being the first CA ever to be removed from browsers' list of trusted roots for weak security.

For 2012 there is only a list of major hacks so far:

Hacks in 2012

CSLEA hack
Occupy Nigeria
Operation Megaupload
Anti-ACTA activism in Europe
Operation Russia
Boston Police Department attacks
Syrian Government E-mail Hack
AntiSec Leak and CIA Attack
Interpol Attack
AIPAC Attack
Vatican website DDoS Attacks
Bureau of Justice leak
Taking down Monsanto's Hungarian website
Symantec source code leak
April 2012 Chinese attack
Operation Bahrain and Formula One attacks
Occupy Philippines
Operation India
Operation Quebec
Operation Japan
Operation Anaheim
AAPT attack
Operation Myanmar

APPENDIX II

Cross-border flow of Internet traffic and interference which may have an impact on access to content, services and applications
Report by Patrick Fälstrom and Gordon Lennox

Background

The Council of Europe in its human rights safeguarding role, particularly the right to freedom of expression (Art.10 of the ECHR), recognized the need to consider the free cross-border flow of Internet traffic in addition to previously other Internet-related approved standards.

The so far debates and scenarios on interferences with Internet traffic across borders revealed that challenges of different nature exists, however additional documented cases have to be identified in order to elaborate an instrument designed to preserve or reinforce the protection of the cross-border flow of Internet traffic. Some potential scenarios/ cases illustrating interferences with Internet traffic across borders and already explored by the CoE highlight two key elements (1) the potential or actual impact on access to online information and (2) the cross-border impact.

The nature of the issue requires a multi-dimension examination: the policies that will be identified should consider both technical and legal aspects.

Cases will possibly examine, but not limited to, matters related to: key stakeholders in ensuring the Internet traffic, the technically borderless nature of the Internet, the distinction between the Internet technical infrastructure and the content that flows on it, explanation of Internet traffic concept, deep packet inspection, routing, filtering, blocking, existence of the Internet borders in terms of jurisdictions, etc.

Additional sources such as the European Court of Human Rights case law on trans-border information transit and Internet governance, the OECD work in Internet related issues, the International Telecommunication Union Regulations should also be examined.

The general objectives of the exercise:

1\ to produce a report in which to document challenges and cases to the unimpeded cross-border flow of Internet traffic from legal, technical and policy perspectives, and to reflect eventual best practices;

2\ to assess the feasibility of elaborating an instrument designed to preserve or reinforce the protection of the cross-border flow of Internet traffic based on the report's findings and the scope of CDMSI;

3\ to recommend elements for such an instrument to be adopted by the CoE Committee of Ministers.

A. Introduction and summary

For many people it is now the cloud. They do not understand it – and why should they? They simply connect to the cloud and then do an amazing variety of things: some important for them as individuals, some important for society as a whole, and much in between. It is difficult to categorise in a new and interesting way what we do in the cloud: it covers almost everything. The details may not be new as Tom Standage showed in his book "The Victorian Internet". But the scale, the intensity, the volume is new.

The curious lack of geography is also new however. People may use different devices to connect: a laptop, a tablet, a smart-phone, their computer in the office or the computer in the corner of reception at some hotel. Once connected though they presume they can continue to access the same services, even if they very often do not know where the services are located. When they wish to communicate with somebody, whether to have a video-chat or send a large document, distance is not an issue. Time-zones perhaps because people still like to sleep. So where somebody is at any moment, where the services they wish to access are: often these are seen as irrelevant. People still want to read their favourite newspaper, send that quick note back to the office, make a medical appointment for when they get home, submit some course work, see and talk to friends and family. So geography and perhaps particularly frontiers have faded significantly from view.

New things continue to become possible though because of the cloud and there seems to be no end to that. But for most people the cloud is nice and neutral. Of course they cannot see inside the cloud but they presume that everything "just works" as it should. And perhaps that is how it should be. So they communicate with who they wish to communicate with, they access the information and the services they feel they need.

However sometimes things do not work as people think they ought to. Some things simply do not work or work badly. They cannot communicate with certain people and they do not know why. And even if they do they are not always certain that other entities are not also silent parties to any communication. Or they cannot access some information or services. And if they do, can they be certain that the fact that they accessed a service or the usage they made of a service is not also being monitored and recorded. Can they indeed be sure that the service they tried to access is actually the service they are now communicating with?

Again some of this is not fundamentally new. But then again very few of us are spies or secret agents!

When things go wrong however, or do not work as expected, when we find ourselves hindered from doing certain things or we find things happening that we did not wish, it can be, and often is, the result of a technical failure or a poorly thought out decision within an organisation. But in the environment we are going to consider it can also be about local policy decisions and particularly local policy decisions that have non-local effects. Indeed as we will see, a person in one place who wishes to access a service in a second place may find that access hindered because of decisions in a third non-obvious place.

In exploring these issues we will not insist on a hard demarcation between what has been traditionally seen as telecommunications and the Internet. While there are differences, and some would say very important differences, it is also clear that the distinctions in many areas are increasingly blurred and this trend will continue. Much, if not all, modern communications uses much of the same infrastructure, technologies, standards and resources. There is not one cable across the sea for telecommunications and another for the Internet. Everybody is using IP – the Internet Protocol - and AS – autonomous system – numbers, and not just for the public Internet. Many people use their smart phone and their mobile subscription as a way of accessing Internet services. Governments in turn look to the more regulated telecoms sector to block or control communications.[1]

The remainder of the report starts with looking at what is involved in what ought to be a simple case: a single user looking at a single web-site. The complexity revealed there however helps us set the scene for the rest of the report.

There is then a more technical look at the various generic aspects of IP networks before continuing by looking at how communications can be blocked, interrupted, or otherwise interfered with, particularly where the effects are caused cross-border.

[1] The stories from the "Arab Spring" are well known but the Irish government recently also felt obliged, in advance of the G8 meeting, which is actually taking place across the border, to ensure that it had the formal powers to block all usage of mobile networks in certain areas in certain circumstances.

The conclusions are then almost self-evident.

The global and local importance of modern communications networks is difficult to underestimate. These networks are also amazingly complex and they are growing even more complex as more systems and services are added.

They rely however on an amazing cooperative and yet decentralised management system. In fact the Internet is amazingly free of traditional formal contracts. When things go wrong, and of course they do go wrong, there is no central office, no chief officer to decide what should be done. Instead thousands and thousands of people, often engineers, working independently take the appropriate actions.

In some ways this should not work. This is not a system set up by any committee. The fact that it does work, that it continues to be capable of both growth and innovation, that it has shown itself remarkably robust, says something positive about humanity.

Such an environment though continues to need shared principles, principles that are clear and coherent and that reflect the technological as well as the social, economic and political realities. This is an obvious on-going task for the Council of Europe.

B. Clouds

Clouds can be pretty. But clouds can also hide things, things it might sometimes be better to know about.

Images of clouds have been used when discussing networks for quite some time. When traditional telecoms companies were selling point-to-point circuits a drawing of a cloud was sometimes used. The cloud symbol helped indicate the provider's domain of responsibility, effectively hid the internal complexity of the network and focussed on the end user.

This was all fine when the product offered was an end-to-end circuit. What went in one end was what came out the other end. Users were expected to be only concerned about their end and the other end and the quality of the circuit in between. So for a while it was only about price and effectively a standard Quality of Service - QoS.

Then along came the Internet...

In the early days of the public web many people presumed that networks continued to work just as telephone networks did. They of course used a telephone circuit to connect to the Internet. And indeed their model was indeed not that wrong. People went to a web site and in a sense they had a connection to that site. They could browse around on that site either by navigating within a page of information or clicking on a link that took them to another page on the same site. Or they would click on a link that would take them to another site - another connection? - and the process would continue.

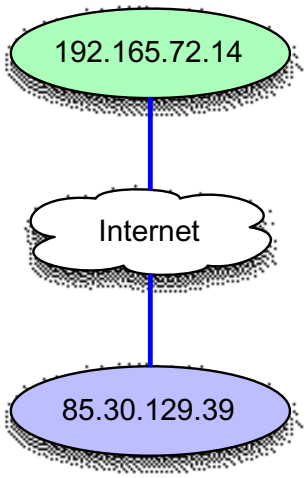


Fig1: Client (green) connecting via HTTP to a server (blue) over the Internet

A lot of the recent discussion though about network neutrality and QoS seems to be predicated on that model. But is it really still good enough? Because the Internet keeps changing. Or more accurately perhaps, people keep using it in different ways.

Now one of the great things about the Internet is that the user can see some way into the cloud and this is what we did. We looked at what happened when a user went to a modern and not so atypical web site. You can try the same thing and "your mileage will vary!" But this is what we saw as we peered a little deeper and deeper into the cloud.

A user types "stupid.domain.name" into their browser.

Now for DNS queries most people's computers off-load some of the work to a "resolver" – another computer, a sort of proxy - on their local access network. For popular domain names the "resolver" will cache the response to previous queries. But given that there are a few hundred top-level domains and many millions of second and third-level domains the majority of domain names are not "popular". So either the user's computer or the resolver fires off in turn queries to a root server - pick 1 from 13 - and then to a TLD (top level domain) server - in this case pick one of the 10 name-servers for .NAME - and then...

In reality the resolution (as it is called) of a domain name to an IP address is a complicated process. In this case, if the name-server chosen for .NAME is c6.nstld.com, then the client must first resolve that name before it can resolve stupid.domain.name. And so it continues in a recursive process until all names involved are resolved to their respective IP addresses.

So there are interactions with about ten name-servers in various domains just to get the address associated with "stupid.domain.name" and the user's computer is ready to do: http://stupid.domain.name/

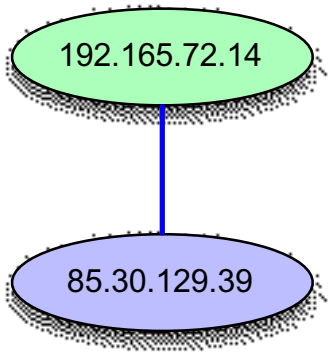


Figure 2: Client (green) connecting to a server (blue) using HTTP (blue line)

Are we finished? Well not quite!

First of all a typical web page consists of multiple objects - chunks of text and various images. So there are local links that result in more http requests to download, for example, the images. And of course there are the passive links to other web pages of the same server or other servers. The user decides whether to click on those or not, whether to go to the other page or not.

But the home page for "stupid.domain.name" also contains a number of active links to content on other servers. To completely and properly display the selected home page these other servers, servers elsewhere and on other networks, also have to be contacted.

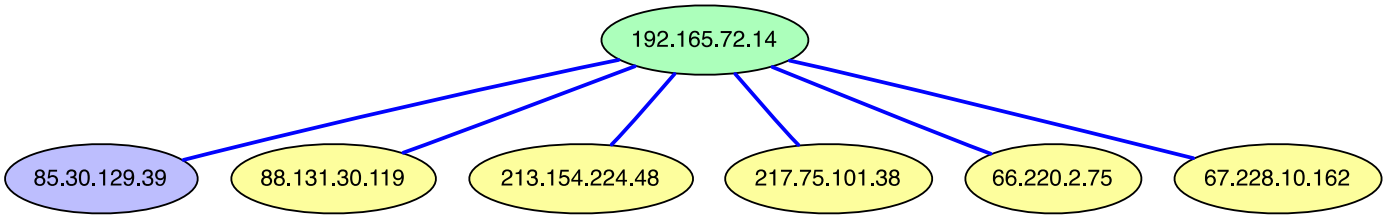


Figure 3: Client (green) connection to server (blue) and additional content servers (yellow) using HTTP (blue lines)

So we have another 5 series of separate DNS resolutions, each resulting in multiple name servers being contacted.

To conclude, to display just the home page of "stupid.domain.name" the client have been in contact with 6 content-servers, and one name-server, which in turn have had interactions with 12 name-servers.

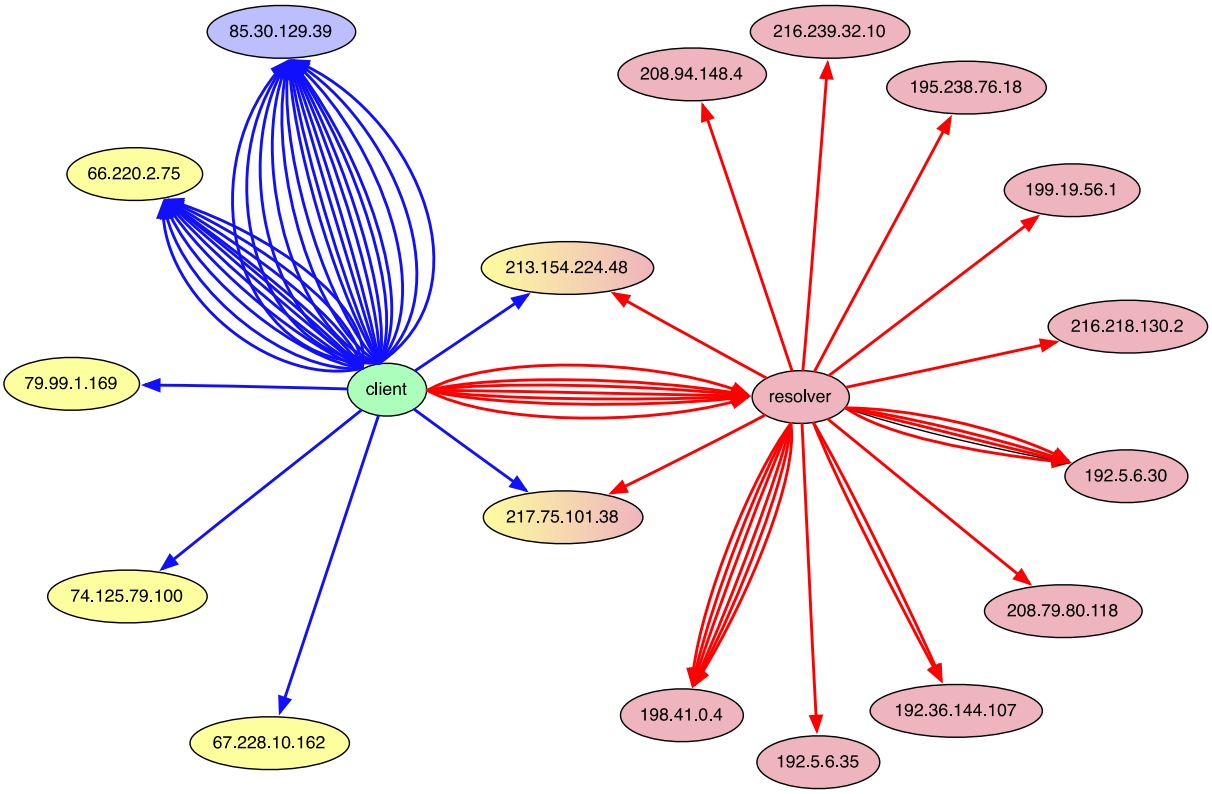


Figure 4: HTTP connections (blue) and DNS connections (red)

This is illustrated in Figure 4 where we see name-servers as red, and content-servers as yellow. The lines indicate transactions either HTTP (blue) or DNS (red). We also see that two hosts act both as name-servers and as content-servers.

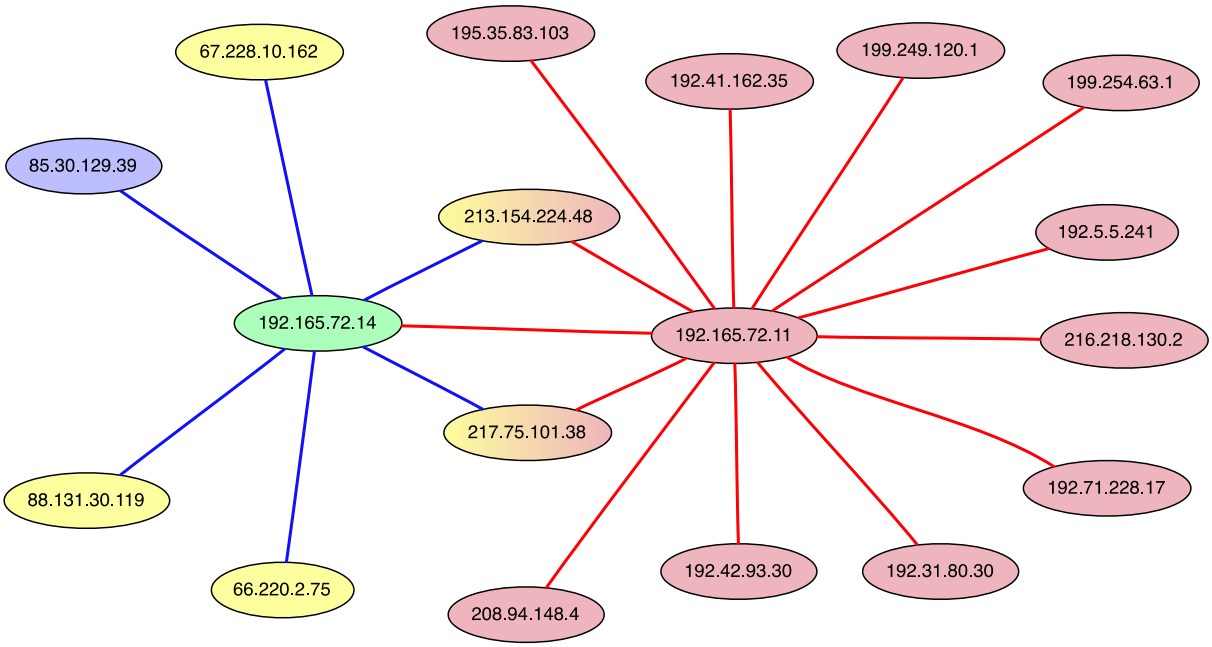


Figure 5: Simplified version of figure 4, only showing connections and not flows

Are we finished?

Well still not quite. We can still peer a bit further into the cloud and still see a bit more. Where are the servers we have mentioned? Which networks are they on? And which intervening networks need to be traversed?

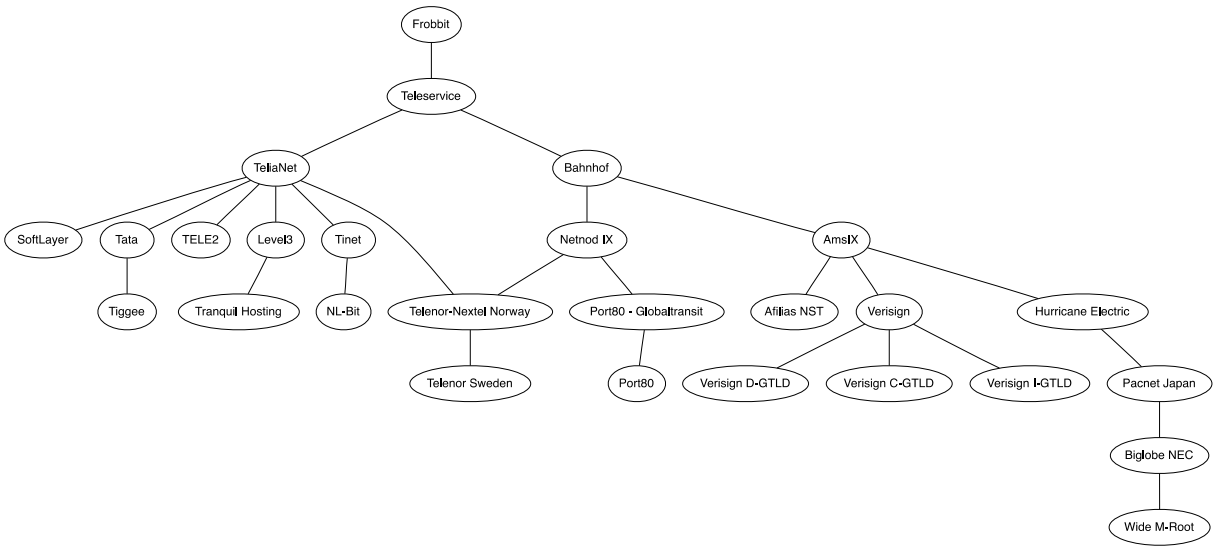


Figure 6: Networks involved when fetching one web page

A bit of playing around and we identified about 27 autonomous networks which are involved either in hosting the servers or providing transit. Are we finished?

Not necessarily. We could probe a little the activities of some of the boxes involved - but obviously not all. There are various "boxes in the middle" doing what "boxes in the middle" do. From routers to proxies, from NAT's to firewalls, from load balancers to content caches, in this specific case more than 100 boxes are involved! And then there are tunnels...

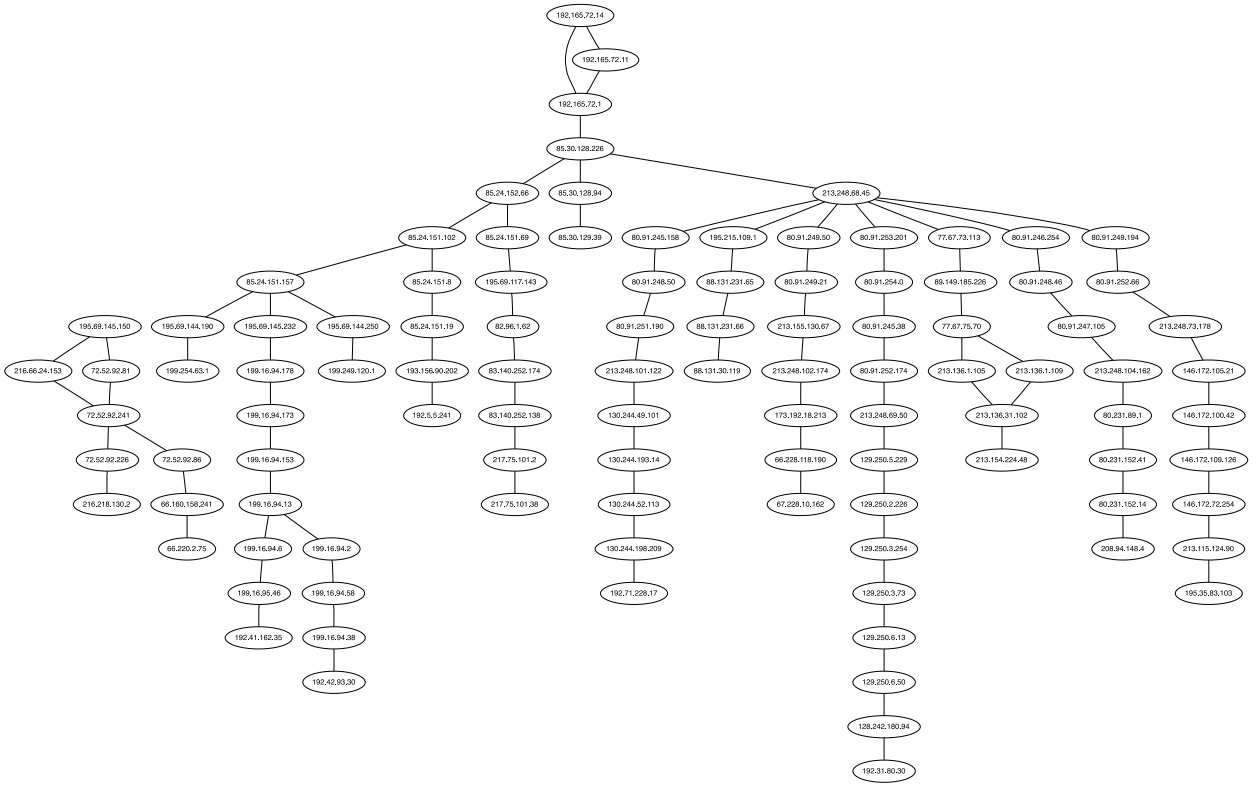


Figure 7: All the boxes involved, boxes acting on the IP layer

But we will pause here.

So in this case one user looking at one home-page involves 17 servers (name servers plus content-servers) scattered across more than 27 networks (hosting and transit).

Of course each of these servers has only so much local access bandwidth and so much processing power. Indeed some content/service boxes will decide unilaterally how much of their resources they will devote to any incoming request. And to state the obvious: your access provider does not have any contract with the average content or service provider.

Anyway our typical user might then just decide that "stupid.domain.name" was not the site they should be looking at right now and decide go somewhere else. So the process would start again. There are potentially lots of places they could now go to though. .EU has well over 3 million domain names registered and .SE has another one million and so on. And again your access provider has contracts with almost none of them. Indeed your access provider probably does not have a contract with either the .EU or .SE registry.

On the other hand the user might just go off and do something else: go for a beer or read a book. The web page is of course "still there". So the "circuits" are still active, still being used? Well no. There were and are simply no circuits in the traditional sense. The DNS in particular is very forgetful. A query comes in and a response is sent back. And the transaction is forgotten. The response may be cached for a while to help with responding to another query from another user. But that is it. The content on the screen? Well that has been delivered. Until the user or their browser requests more content or some content needs to be refreshed there is no further interaction with the content server. So there is no need to shut down the browser before reaching for that beer and a book.

This glimpse into the cloud should hopefully have helped in understanding a bit of what is going on now and why traditional notions like circuits and some current suggestions about QoS are not quite what they seem. They just do not make sense anymore. You cannot buy a circuit with a defined QoS to

any web site of your choosing. You do buy connectivity into the Internet - the cloud? - and that allows the mass of interactions that are needed even to just look at a simple web page these days.

The image of a cloud remains useful. And even pretty. But we have to remember sometimes what is inside. And what may be inside.

C. The Internet and other IP networks

All communications networks today are computer networks, whether those computers are mobile-phones or huge server farms. Services rely on data being exchanged between a number of computers or devices, and many more than the average user might imagine.

At its simplest an end user often may some human friendly name (often a URL, which include the hostname of the server). The DNS is then used to get the IP addresses related to the host name and requested services, and finally the devices identified by the IP addresses communicate.[2]

So various pairs of devices send packets to each other. Each packet includes a sender and a destination address, together with a few other identifiers that say what application is involved. This implies we do not in reality have any permanent connections. At least not compared with "traditional" telecommunication where a circuit was allocated, together with resources that would be enough to carry on the communication.

Instead each packet includes enough information so that devices that see the packet during transport know the sender and receiver. This is used by so called *routers* that connect networks to each other to know which one of a number of alternative networks a packet is to be forwarded to. Networks obviously vary enormously in size and so do routers. A domestic or home network will have a small router between it and the network of the access provider. Organisations, large and small, may have multiple networks and many routers.

The routers are configured with information about what networks they are connected to and which end addresses can be accessed via those networks. Such routing information is often exchanged dynamically between neighbouring routers. so that every router on the Internet can know in what direction to forward a packet that is under transmission. To keep things simple though, particularly on small networks, there will be a default. Any packet destined for an address not explicitly known by the router will be sent to a specific other network. The default for a home router will obviously be the access provider's network. In addition very large routers, routers which do not have a default route, may simply discard packets if they do not have explicit information on how to forward a packet.

So networks consist of very many boxes with links between them. The boxes include computers of all kinds, routers, which are just specialised computers, and other kind of equipment (like switches). Those physical connections or *links* and need not only consist only of cables (of optical fibre or copper) but also radio links. One exceptionally common type of link is that between a cell phone and the radio tower it currently is attached to. Cross-over phones will then pick between the radio links available – for example WiFi at home and 3G when away from home.[3] Other common types of link are copper wires (Ethernet, various DSL technologies and so on) and fibre (from transoceanic links to various FTT* mechanisms such as Fibre to the Home or FTTH).

All networks together therefore involve a huge number of different components. Some kind of structure or architecture is required to provide the necessary levels of abstraction. The following model is useful here. It should be noted that other descriptions and models are possible.

---

[2] It is often stated that in the beginning the DNS was all about providing user-friendly names rather than numbers as humans were not supposed to good with numbers: this is not exactly true!

[3] Indeed some smart-phones will vary the services they allow based on whether they are roaming or not.

- Links of various kinds, fibre, copper, radio
- Active equipment the links are connected to, such as switches and radio towers
- Networks, composed of links and active equipment
- Routers that connect networks to each other
- IP packets that are the actual payload of the communication
- Routing is the control protocol between routers that instruct them where to forward IP packets
- DNS that, at its simplest, maps domain names to IP addresses
- Applications that give the end user the experience sought

1. Networks and IP addressing

Each device directly connected to the Internet needs a globally unique IP-address. The format of the address depends on which version of the Internet protocol (IP) is used. In IP version 4 (IPv4) the length of the addresses is 32 bits, in IPv6 it is 128 bits. The length of the address, and the version of the protocol is not important for this discussion, so unless explicitly mentioned what is described is valid for both IPv4 and IPv6.

To be able to know in an effective way where topologically a specific device with a specific IP address is the whole address space is divided into subnets - subnetworks. Each subnet can in turn be divided into subnets. Each such subnet is a contiguous series of addresses from the full address space.

One network with IPv4 can for example have a subnet with the address range 1.2.3.0-1.2.3.255[4]. This subnet has 255 addresses and because of this approximately the same number of devices can be connected[5].

The routers that sit between networks keep track of enough of these subnets and address ranges so that when a packet is received, it can send the packet out on the interface that is appropriate for the final destination.

The physical area a network covers with its links can be large. Even very large, and cover large areas of earth. Examples of large networks are the ones that have links that cross the Pacific Ocean, Europe or go around Africa. Smaller networks are for example the ones in people's homes, or between people's cell phones and computer when the cell phone is "used as a modem".

It should be explicitly noted that there is nothing that prohibits a network to have links that crosses boundaries between countries. In fact, for global Internet Service Providers that is rather the norm as such global ISPs being active in many countries have a network that covers all of them.

2. Routing

Every router in the world cannot be configured with information about every subnet there is, and where it is. If nothing else, new devices are connected all the time, links break and the path between two devices might change, for example when the devices are disconnected from one connection to a network to a different connection to a different network.

Information about where subnets are located in network terms can be either configured statically in a router or by having routers dynamically communicate with each other. This communication between routers is done via so-called routing protocols.

[4] IPv4 addresses are written as four base-10 numbers, each describing one octet (8 bits) of the 32 bit address. Because of this, each number can have a value between 0 and 255.

[5] In reality two addresses are always "lost" in a subnet, the first and the last. Because of this, the number of maximum number of devices in the example is 253, including the router(s) that are connected.

Given that the router has the necessary routing information; it can calculate a *forwarding table*. This can be viewed as a mapping from a subnet to the interface the packet is to be forwarded on, and potentially because of this a reference to what network will finally receive the packet.

Let's take an example. A packet with sender address 1.1.1.1 arrives on interface 1. The destination address is 2.2.2.2 and the router know that a network to which that address belong is connected to interface 2 because it is statically configured. The router sends the packet out on interface 2.

In another example, the router with name A is connected to network 1.1.1.0 and 2.2.2.0 while router B is connected to network 2.2.2.0 and 3.3.3.0. Router A is not connected to network 3.3.3.0 and router B is not connected to network 1.1.1.0. But by exchanging information between A and B using a routing protocol, A can inform B about the existence of network 1.1.1.0 and B can inform A that network 3.3.3.0 exists. A node on the network 1.1.1.0 with the address 1.1.1.1 can because of this send a packet to a node on the network 3.3.3.0 with the address 3.3.3.3 by first sending it to router A, that sends it to router B that can send it to the intended destination.

But all routers are not connected to all networks, and do not even include routing information for all subnets on all networks. One way to deal with this is for the router to have one special entry in the forwarding table called *default route* that is an entry with information about where all traffic is to be sent when no explicit information exists about the destination.

3. DNS

Just using IP addresses when communicating is though quite cumbersome. For the end user it is complicated to remember IP addresses. It is also complicated to have IP addresses in configurations of computers and applications. The reason for this is not only because "words" are easier to remember than "numbers". It is also because (as explained above) the IP addresses are allocated according to network topology. If a computer move, or if a service move from one computer to another, it might not be possible to keep the same IP address for it.

An abstraction layer is needed, and this is where the Domain Name System (DNS) is involved.

The DNS is both a protocol and a naming scheme. If we start by looking at the naming scheme, it is a strictly hierarchal naming scheme with the most significant token to the right, and less significant to the left. Each name (or domain as it is called) has an authoritative manager, and that manager can either directly allocate names in that domain or delegate subdomains to others. Such delegations can happen (but do not have to happen) at every location in a full domain name where there is a dot ('.').

The DNS namespace effectively starts at *the root* that is written again as a simple '.' although in many cases this is not explicitly spelled out at all. The domain name <<*www.example.com.*>>is often written as <<*www.example.com*>> (without the final '.'). The management of the contents of the root, the root zone itself, lies with ICANN a not-for-profit organisation incorporated in California, USA. ICANN implements the policy for delegation of domain names from the root which results from their policy development process. Examples of such delegations include *com*, *uk* and *se* to various organisations.

Delegations from ICANN are to authorities, often private-sector organisations also called *registries*. Each such registry can then create rules and policies for delegations from their domain name, as long as their local policy is consistent the rules they have promised to follow given agreement with their so-called *parent* (from where their domain was delegated). Many registries have implemented competition regarding registration services by introducing *registrars*. If somebody, an organisation or private individual, wants to register a domain name in a particular domain where registrars exist they can contact an accredited registrar and request delegation, normally by paying a fee and signing an agreement.

Finding an IP address (or other data) given a domain name, involves something called *resolution*. Resolution basically happens top down in the namespace, by issuing and reissuing the same query to a number of name servers. Queries are first sent to one of the root servers, one of the name servers for the root zone. They, like any name server, either respond with the response, or a referral to a different name server, where the query is reissued.

So normally a query will be sent to a root server and then to a TLD (top level domain) name server and then to a name server for the target domain. However the response to a DNS query can also be another domain name and so the process may need to be repeated.

To optimize the querying process, caching involved. Clients, such as end users in enterprises or customers of an access provider, often send their queries to a full service resolver that does caching. This resolver, hosted by the enterprise or by the access provider, normally resides close, in terms of network topology, to the client. More recently service providers, like Google, have launched resolver services, and the assumption that the full service resolver is close to the origination of the query is no longer correct.

One more feature with the full service resolver apart from caching is carrying out the validation of DNSSEC signed responses. DNS responses may be signed with digital signatures that allow the validation of both the administrative origin of the response and that the response has not been changed during transport.

4. Application

On the application layer communication happens between obviously at least two or normally many more end points. All end points involved do have associated unique IP addresses and in this document we use the following terminology:

- Client: a party that initiates the communication
- Server: a party that responds to a request from a client
- Session: one or more requests/responses (or *flows*) on the application layer between one client and one server
- Flow: a series of IP packets using one of the IP protocols (such as TCP or UDP) identified by the 5-tuple {src ip, src port, dst ip, dst port, protocol}

As explained previously, a client fetching one web page might open many sessions, each consisting of at least one flow, over both UDP and TCP, to many different servers.

It is worth remembering however that many of the interactions necessary for this to be possible happen independently of what any particular client or server does. Both BGP announcements and DNS updates happen all the time. Both routing (such as the BGP protocol) and DNS are simply other application layer protocols, using flows, just as http and https are the protocols used for the web. In addition "pull" can become "push". Instead of a client seeking information the server can initiate the communication.

It should once again be pointed out that as each packet includes both the sender and recipient IP address, packets in a flow might be sent using different paths, and might even be dropped (not reach the destination).[6] Protocols like TCP or others on the application layer can manage packet retransmission if that is required, but many applications can handle a certain number of packet drops and still give an acceptable user experience.

[6] Perhaps more commonly the packets going in one direction may follow a different path to packets going in the other direction.

D. Interruption and other forms of interference

One can say that all communication on the Internet consists of one or more flows by end devices, associated with unique IP addresses. Interruption of traffic implies that a third party somehow blocks or diverts or changes one or more of the flows between end devices, and does that in such a way that the information sought does not reach the client or the required service is unavailable or compromised.

Blocking can be done on multiple layers of the Internet architecture. The effectiveness of the various mechanisms has been discussed elsewhere and the only thing that there is agreement on is that blocking will always have secondary consequences. The questions are rather *why* the blocking happened, *what* problem, if any, was to be solved and *whether* the chosen method was sufficiently precise to solve the problem and any secondary consequences are either minimal or at least proportionate.

SAC-050[7] discusses specifically the differences that exist on whether the blocking has secondary consequences outside of the administrative area for which whoever decides on the blocking is responsible. Elsewhere this document specifically looks at the special cases when the secondary consequences cross country boundaries.

It should also be pointed out that blocking may be a conscious decision by whoever is doing the blocking. That decision might in turn be based on action by law enforcement agencies, or decision-making processes based on contractual agreements (misuse, lack of payments, etc).

But it can also be blocking by mistake. A simple configuration error, or bug in the provisioning software might create the same kind of technical implications as a conscious decision. Because of this, design of solutions should be robust enough that mistakes in configuration and management will tend not have blocking implications.

1. Traffic

Complete blocking of traffic is both easy and hard. Examples include a cable being cut, wireless access being disturbed, a device being simply unplugged, or essential services a device needs for operation (such as electricity) being disabled.

It can be easy if one knows which device should not communicate, one can target actions at that specific device, either the device itself, or by blocking all traffic to and perhaps from the specific IP address of the device, whether client or server.

This blocking will not work if there are alternative routes between the two parties that do not implement the required blocking.

Traffic blocking must because of this happen very close to either of the devices that communicate. But if the services available are replicated on more than one device (for example using anycast services) traffic might be able to reach one of the alternate nodes.

So, the simplest way of blocking traffic is to target one of the end nodes. Then the further from the end nodes one gets, the harder it gets to block only that communication and nothing else. For example, inspection of IP addresses of every packet is needed to block traffic to or from a specific IP address.

There is however also the problem that very many devices do not have their own public IP address: they are behind a NAT – a network address translation device. Blocking traffic to and from the public address in this case will have immediate secondary effects, which may go as far as blocking many or all devices behind the NAT.

[7] http://www.icann.org/en/groups/ssac/documents/sac-050-en.pdf

2. Routing

Routing can be used indicate that a destination is unreachable so that no attempt is made to forward traffic or to divert traffic away from the intended destinations so that it can be discarded or delivered to alternative systems.

So either an authoritative source of the route announcement stops announcing the network (withdraw the announcement) or a third party announces a more specific prefix (that includes the IP address to be blocked).

The first will remove the ability for parties to send traffic to the blocked service.

The second will redirect traffic intended for the blocked service to reach instead someone else. This is achieved, either accidently or deliberately, by announcing an address or network prefix with a specific destination and doing it in a way so that the announcement is trusted among the listeners, and ensuring that it gets higher priority than the real announcement.

3. DNS

The DNS has two different information paths where blocking can happen. On the registry side the domain name can be removed from the zone file. On the resolution side certain resolvers can be programmed not to resolve the domain names in question.

DNS blocking is described more in SAC-056[8]

There are two counters however. Content can be made available under another domain name. Users can use alternative resolvers. Access providers may try and block access to alternative resolvers but then there are possible ways around this. Escalation as usual?

4. Applications

Blocking specific applications is normally by blocking specific port numbers, or by inspecting packets using deep packet inspection or other mechanisms, and then packets that match a specific policy are simply dropped.

Application layer blocking is quite often discussed in the context of *Network Neutrality*.

However again there are counters in some cases. Proxies may be used. That is a computer elsewhere can act as a go-between. Alternatively encryption can be used. This effectively "hides" the content. These techniques, proxies and encryption, can again be combined to offer more possibilities to communicate in the presence of certain kinds of blocking.

Blocking encrypted or secure traffic is still possible. But there are various circumstances when encryption is always desirable. For an access provider to automatically block such traffic implies significant side-effects.

The most common form of application level blocking is of course the blocking of e-mail which is considered as "spam". Spam filters can act in various ways and at various levels. Filters can act at the level of IP address blocks but that tends to be quite extreme. More normally filters operate at the level of domains, e-mail addresses and of actual e-mail content. Some filters are operated by third-parties and some use information from third-parties. All e-mail service providers use them. And of course individual users use them.

[8] http://www.icann.org/en/groups/ssac/documents/sac-056-en.pdf

Filters have their side-effects of course. They are not perfect. Blocking a domain blocks all users using that domain. When at the other extreme decisions are based on content of individual items then a choice needs to be made as to whether the filter should be set at a stronger level where not only all suspected spam is blocked but also some acceptable and desired mail is blocked or at a weaker where some spam is acceptable in return for being reassured that "good mail" will not be accidently.

Such filters can also be used politically or be subject to local regulation. There is potential for problems here in that very many people use non-local mail services. The filters and indeed aspects such as data protection or retention or the possibilities fir interception may not always be what they might expect and of course are ultimately subject to political and legal controls which are not local

E. Cross border implications and effects

To a first approximation traffic follows the line of least financial resistance. This has meant that in the past traffic even between two end-points in the same country may have actually left the country at one stage or another. More recently, and perhaps it is still not that unusual, traffic between two neighbouring countries may actually transit through a third country.

In addition actually identifying or locating an end-point in the same country may involve services administered and hosted elsewhere in other countries.

At the same time it is increasingly difficult for users, even expert users, to know what is happening where. Content requested from a service far away may actually come from a content-server which is quite close. Or content may be acquired from a peer2peer network which can be quite dynamic.[9] A DNS query may go to some anycast server. These are servers which are effectively clones of some master server and which exist in various places while each instance has the same IP address. Or the query may go to a secondary server which is again a copy of the main server but this time has its own different IP address. And all this before we even consider technologies such as TOR.

1. Traffic

Blocking traffic has cross border implications if the location where the blocking is happening is not in the same country as at least one of the two ends that communicate.

This can happen if for example an ISP (that carries traffic) is covering countries A, B and C and a decision in country B forces the ISP to block traffic from B to a site in country C. So a decision in B affects not only people in B but also an entity in C. This might very well also impact traffic to the site from country A, particularly if traffic from A transits through B to C.

The blocking might be very difficult (or expensive) to implement without having the ISP split the network in three, so that it only needs to implement the blocking in country B. But it may also involve the ISP buying separate transit to by-pass B. and all this for one site?

2. Routing

Blocking using routing is probably the most commonly blocking that happens today, and that in most cases by configuration mistakes. One of the more well known cases was when Pakistan Telecom started an unauthorized announcement of the address block used by YouTube. The announcement was supposed to block YouTube locally in Pakistan but was leaked by being re-announced by PCCW Global, and it ended up blocking access to YouTube across a wide region.[10]

[9] While P2P networks have had a bad reputation they also represent an remarkably cost-effective way of distributing data and as such they have been used by NASA and the EBU, among others.

[10] https://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

3. DNS

Removing domain names completely by either contacting the registrar or the registry is quite common, although the effect is questionable, and depends on what the real problem to be solved is. It is not that unusual though for the administrative and commercial chain to be very international. And that can even be more so if somebody wants to make things complicated.

So ICANN in country A delegates a TLD to a registry in country B who has an accredited registrar in country C and it is that registrar that a registrant from country D chooses. But the web-site, for example, is hosted in country E and the primary users of that web-site come from country F. There is an immediate and obvious question of jurisdiction. It might be easier of course if at least the registry and the problem are in the same jurisdiction.

Today quite a number of take-downs are happening according to the legislation where the registry resides, even if the parties communicating are not within that jurisdiction. So as just one example, there was the requested take-down in the US of a domain name for a domain name registered in Canada for a gambling site.[11] In Europe

The problems are going to get much worse. In the past a almost all TLDs were country code TLDs with the implication that there was a relationship between the code and a local jurisdiction. With the vast increase in TLDs planned all the new TLDs will all be effectively registered directly in one jurisdiction: California.

Blocking or redirection based on individual queries to DNS resolvers is very common. It is carried out by various actors, sometimes at the user's request, and sometimes according to the policy of the access provider and by an access provider following requests from the local authorities.

One might consider that these have no bad cross-border effects as they are effectively locally. While some might see a restriction on cross-border commerce, for example, others would argue, perhaps rightly, that this can be a legitimate goal. There is the twist though that as people can often choose their resolver, even if they do not normally exercise that choice, they can also choose to evade or ignore the local policy and instead choose another.

DNS Changer was a particular case where malware was used to change the resolvers used by a number of PC users to redirect their queries to some particular name-servers.[12]. The possibilities for doing harm by the operators of those name-servers was then significant. Action was rendered legally more feasible because some of the victims were in the same jurisdiction as the servers. However simply taking down the servers would have meant a number of people, and nobody knew how many or where they where, would effectively lose their Internet service. So an interesting an highly skilled technical exercise was required.

4. Applications

Application layer blocking is often discussed when talking about network neutrality. Such blocking is often due to business models. This has been the case when blocking VoIP traffic and in particular Skype. Such blocking may have the backing of a state either because they favour the local business model or for other reasons such as national security.

Regulation is sometimes then used to remove a block. One famous example is the blocking of VoIP by MadisonRiver in 2005[13], but many other examples exist.

---

[11] http://blog.easydns.org/2012/02/29/verisign-seizes-com-domain-registered-via-foreign-registrar-on-behalf-of-us-authorities/

[12] http://www.circleid.com/posts/20120327_dns_changer/

[13] http://www.cybertelecom.org/voip/blocking.htm

But of course sometimes regulation also is used to add a block, such as the order in Denmark to Tele2 to block access to The Pirate Bay[14].

Such blocking tends to be local in application and effect. It affects primarily local users, even when in some cases it could be argued that it also may affect cross-border commerce.

The major common cross-border application though has been and remains email even if applications such as Twitter and services such as Facebook are obviously seen as very important by all those who use them. All of these have been and are subject to blocking and filtering. Some decisions are of course made by the remote service provider and some are made in their home jurisdiction and some again by the local access provider and by their local regulatory authorities.

F. Conclusions

Communicating in the presence of certain forms of blocking is in some ways and for some people just another technical challenge. Enforcing blocking is however both a technical and a legal challenge.

Blocking is though only one way to interfere with communications which may not be desirable by those communicating.

Communications may be redirected. For example an attempt accidental or otherwise to access content or services on the web may result in the user being redirected to a "warning page" if the original content was believed to be either illegal or present a security risk. But as we have seen redirection can also result in people being redirected towards a dangerous site.

As we have also seen however accessing content or services can be implicit. The user thinks they are going to one site when they are actually going to several at the same time and not only are some of those sites not under the original site owner's control the choice of those additional sites is not theirs either. There is therefore a curious mess of desired outcomes and policies.

An interesting aspect of the "arms war" here is that while web-sites are increasingly using digital certificates to allow the verification and validation of the required access parameters there are already indications that states are beginning to use fake certificates so that people have a false sense of security while still being redirected.

While redirecting a user to a warning page may be useful or even simply benign, the redirecting or compromising a software update process could be catastrophic.

The other major concern is of course "eaves-dropping", but on a massive scale. Traffic in transit is often considered "special": available locally but not actually domestic. So there can be different rules. This has always been a concern but it has very recently been in the headlines again.

Blocking may though be done for a wide variety of reasons: to block access to undesirable content or services, to block access to illegal content or services, to block access to content or services for commercial reasons, to block access to content or services on the grounds of public order or national security.

Disrupting the communication links of the adversary has been one of the first objectives in times of war, just as has maintaining communication with those in the other territory. Where people cut telegraphic cables they now cut optical fibre. Where people used clandestine radios they now try and supply or maintain more current forms of communication capacity. This remains a strategic concern for many even if perhaps a little out of scope here.

[14] http://torrentfreak.com/pirate-bay-blocked-by-isp-080204/

In many cases conventional blocking, no matter who the instigator is, has a local intent to deal with a local problem and will have primarily a direct effect. However some forms of blocking have greater potential for cross-border effects.

If an organisation blocks access to certain forms of content and services to those it employs while they use its network, if an access provider blocks access to certain forms of content and services by its direct customers; if the government decides to request the blocking of access to certain forms of content and services then there are certain criteria against which such blocking could reasonable be expected to be judged. These include the freedom of expression, the right to privacy and so on. One might then rightfully expect a degree of clarity on the policies being enforced.

Blocking at this level, no matter how it is implemented, may be considered to have no significant cross-border effects. It is of course liable to lead to user confusion and frustration as they struggle to understand the difference between what they can do and when they will be monitored, whether in the office, or when using the office laptop or their own computer when at home, or when using their smart-phone either on 3G or on WiFi, or when using various WiFi networks somewhere else.

Other forms and styles of blocking or other interference can have significant cross-border affects. This is potentially the case where the user and their access provider are in one jurisdiction and they make use of services elsewhere under other jurisdictions. It is more insidious when the average user is not aware that they are using services elsewhere.

The problem is increased when regulators courts see blocking of particular services as an easy solution to a local problem without understanding the wider context and most particularly the impact of their decisions elsewhere.

The two key areas identified as significant in the cross-border context are are the services to do with the DNS and with transit. There is a third which is growing in importance and that is the area of digital credentials.

These are areas where the Council of Europe could work towards increased clarity and coherence across countries.

Modern communications rely on diversity and duplication to deliver robustness and reliability. Blocking and filtering may sometimes seem desirable but they can also artificially constrain activities to the point of fragility and trust being lost. As in so many things clarity and well-informed decisions are required.

APPENDIX II

Cross-border flow of Internet traffic and interference which may have an impact on access to content, services and applications
Report by Professor Yaman Akdeniz, Faculty of Law, Istanbul Bilgi, University, Turkey[1]

Introduction

The Council of Europe in its human rights safeguarding role, particularly the right to freedom of expression, recognized the need to consider the free cross-border flow of Internet traffic in addition to previously other Internet–related approved standards. The Resolution on Internet governance and critical Internet resources[2] invited "the Council of Europe to explore the feasibility of elaborating an instrument designed to preserve or reinforce the protection of the cross-border flow of Internet traffic."

Furthermore the Committee of Ministers of the Council of Europe adopted in March 2012 the CoE Strategy for Internet Governance 2012 -2015[3] which stated that "an open, inclusive, safe and enabling environment must go hand in hand with a maximum of rights and services subject to a minimum of restrictions and a level of security which users are entitled to expect. Freedom of expression and information regardless of frontiers is an overarching requirement because it acts as a catalyst for
the exercise of other rights, as is the need to address threats to the rule of law, security
and dignity."[4]

The CoE Strategy for Internet Governance 2012 -2015 identified priorities and sets goals for the next four years (2012-2015) to advance the protection and respect for human rights, the rule of law and democracy on the Internet. Its main objectives include:

- protecting the Internet's universality, integrity and openness;
- maximising rights and freedoms for Internet users;
- advancing data protection and privacy;
- enhancing the rule of law and effective co-operation against cybercrime;
- maximising the Internet's potential to promote democracy and cultural diversity;
- protecting and empowering children and young people.

The strategy will span two biennium Council of Europe budgetary cycles (2012-2015) and will focus on the delivery of appropriate legal and political instruments and other tools, such as industry guidelines and manuals, through relevant bodies and actors of the Council of Europe (steering committees, groups of experts, monitoring bodies, commissions, etc) as well as through co-operation arrangements between governments, the private sector, civil society and relevant technical communities.

---

[1] Yaman Akdeniz' recent publications include Internet Child Pornography and the Law: National and International Responses (London: Ashgate, 2008: ISBN: 0 7546 2297 5), Racism on the Internet, Council of Europe Publishing, 2010 (ISBN 978-92-871-6634-0) and Report of the OSCE Representative on Freedom of the Media entitled Freedom of Expression on the Internet: Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States (2011). For further information about his work see <http://cyberlaw.org.uk/about/>. Akdeniz can be contacted at yaman.akdeniz@bilgi.edu.tr.

[2] Adopted by the ministers of states participating in the 1st Council of Europe Conference of Ministers responsible for Media and New Communication Services, held in Reykjavik on 28 and 29 May 2009.

[3] See CM(2011)175 final, 15 March 2012.

[4] Ibid, para 3.

So far as the Protecting the Internet's universality, integrity and openness heading is concerned, the CoE Strategy for Internet Governance 2012 -2015 stated that "the global success of the Internet is owed to the fact that it is open, non-discriminatory and easily accessible. The maintenance of the structure requires the progressive development of international standards that are mutually recognised by states, the private sector, civil society and other relevant technical communities." Action will therefore focus on:

a. developing a "framework of understanding and/or commitments", based on the Council of Europe's core values and principles on Internet governance to protect the Internet's universality, integrity and openness as a means of safeguarding freedom of expression regardless of frontiers and Internet freedom;
b. exploring the possibilities for enhancing access to the Internet to enable the full exercise of rights and freedoms;
c. developing appropriate human rights-based standards to protect and preserve the unimpeded cross-border flow of legal Internet content. This includes ensuring that the Internet is, at all times, accessible and without any arbitrary interruption (i.e. not "switched off") by fostering inter-state (international) co-operation so that governments can better anticipate, prepare and thereby avoid disruption to the Internet;
d. promoting Council of Europe human rights standards globally and, in this respect, encouraging member states to bear these in mind in their bilateral discussions with third countries, and, where necessary, consider the introduction of suitable export controls to prevent the misuse of technology to undermine those standards;
e. developing human rights policy principles on "network neutrality" to ensure Internet users have the greatest possible access to content, application and services of their choice as part of the public service value of the Internet and in full respect of fundamental rights.

The Steering Committee on Media and Information Society (CDMSI), which functions under the authority of the Committee of Ministers, has a main focus upon the oversight of the Council of Europe's Strategy on Internet governance 2012-2015 and the preparation of specific instruments involving the Internet. Specifically, the CDMSI Terms of reference[5] foresees among the 2013 results an "instrument on cross-
border flow of Internet traffic".

The CDMSI at its first meeting, in March 2012, had agreed to consider output on the basis of a preliminary report identifying concrete issues related to the Drafting of an instrument on cross-border flow of Internet traffic. Consequently the CDMSI Secretariat prepared and presented "*The Preliminary report on scenarios of interference with Internet traffic which may have an impact on access to information across borders*"[6]. The preliminary report recommended that "the Secretariat should also explore the possibility of preparing an expert report which analyses legal, policy and technical issues of cross-border flow of Internet traffic and examines policy options to be pursued."

The nature of the issue requires a multi-dimension examination and the potential policies that will be identified should consider both technical and legal aspects.

Key Concepts

An assessment on the feasibility of elaborating an instrument designed to preserve or reinforce the protection of the cross-border flow of Internet traffic will be provided in this report. A number of key concepts are identified in the Preliminary report on scenarios of interference with Internet traffic which may have an impact on access to information across borders[7]:

[5] http://www.coe.int/t/dghl/standardsetting/media/CDMSI/CDMSI_Mandate_en.pdf

[6] See CDMSI(2012)015.

[7] See generally CDMSI(2012)015.

Internet traffic: Internet traffic is the volume of data packets flowing on Transmission Control Protocol (TCP) and the Internet Protocol (IP) which enable the exchange of data between two or more machines connected to the network. Content is an attribute associated with data packets sent across the network. For purposes of this preliminary report Internet traffic is understood as the content and information carried by data packets which travel across the network.

The cross-border dimension: The open nature of the TCP/IP enables interconnection among independent computers and information systems. Internet user requests for any particular content or information can be routed via different servers, which may be located in different countries. This can change at various points in time. Thus, Internet traffic is distributed across borders.

The Preliminary report stated that Internet traffic in one country may be exposed to undue interference by other countries or to actions taking place within their jurisdictions– e.g. country A or action taking place within that country may have an impact on the Internet traffic in country B. This may result in cross-border implications for access to content and information carried by that traffic.

Role of states: Under the European Convention on Human Rights (ECHR) states have the obligation to secure to everyone under their jurisdiction the protection of the right to freedom of expression, including the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers (Article 10 of the ECHR).

Technical (routing) incidents: Internet Service Providers (ISPs) rely on information provided by other ISPs regarding the most efficient route for the data packets to reach their destination. ISPs usually trust the information provided by other ISPs to be correct. Erroneous or bogus announcement of information by ISPs can propagate in an international scale and affect access to specific content or services.

One example is the 2007 incident with YouTube where a decision of Pakistani authorities to block this website resulted in routing errors which blocked access to this website worldwide. Another incident happened in April 2010 when China Telecom advertised erroneous traffic routes which reportedly resulted in 15% of the global traffic being routed through destinations in China although in this case there were no reports on access to any particular Internet content being denied.

Filtering and blocking: ISPs enter into peering agreements and transit arrangements with providers located in different jurisdictions. When ISPs apply filtering measures to connections provided to their peers, the capability of customers (users) of the latter to access to online content may be affected (upstream filtering). Thus, restrictions on content in one jurisdiction may have an impact in another. The Citizen Lab at the University of Toronto has documented one such case[8].

Blocking access to a particular website (either by means of IP address or URL blocking) can have an impact on the Internet traffic to that website on a global scale (web traffic blocking). Reportedly a recent blocking of a content storing and sharing website (MegaUpload) affected significant parts of web traffic in different countries[9]. Content blocking via the Domain Name System (blacklisting websites and filtering IP traffic) also exists, for example by erecting national firewalls, which risks to balkanize the Internet[10].

[8] See Routing Gone Wild: Documenting Upstream Filtering in Oman via India https://citizenlab.org/wp-content/uploads/2012/07/08-2012-routinggonewild.pdf.

[9] See http://gigaom.com/2012/01/20/follow-the-traffic-what-megauploads-downfall-did-to-the-web/

[10] See Advisory by the Stability and Security Advisory Committee of the Internet Corporation for Assigned Names and Numbers: Advisory on Impacts of Content Blocking via the Domain Name System http://www.icann.org/en/groups/ssac/documents/sac-056-en.pdf

Scanning and monitoring Internet traffic: If the conditions of Articles 8 and 10 of the ECHR are not respected, Internet traffic scanning and monitoring raise questions regarding Internet users' privacy protection and in turn their freedom online. There are reports on legislative initiatives in Council of Europe member states allowing for Internet traffic monitoring. The use of deep packet inspection (DPI) technologies also raises questions as regards the legitimacy and proportionality of such usages[11].

Network neutrality: The Declaration of the Committee of Ministers on network neutrality states that "[u]sers should have the greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice. Such a general principle, commonly referred to as network neutrality, should apply irrespective of the infrastructure or the network used for Internet connectivity[12]".

The Body of European Regulators for Electronic Communications (BEREC) released the results of an investigation into traffic management and other practices in Europe. According to the BEREC report specific practices such as blocking peer-to-peer traffic or voice over IP could create concerns for end-users access to online information. BEREC's findings provide analytical data on traffic management by country; they do not seem to cover actual or potential implications of such practices for access to content and services across borders.

Expert Report

Based on this background this report will provide an assessment of legal, policy and technical issues of cross-border flow of Internet traffic, in particular with special reference to the European Convention on Human Rights and the relevant jurisprudence of the European Court of Human Rights. The report will further assess possible policy options to be pursued at the Council of Europe level.

Cross Border Nature of the Internet

The Internet as the largest communication network in the world is increasingly becoming indispensable for everyone around the world to take part in cultural, social and political discourse. The Internet "enables people to have access to information and services, to connect and to communicate, as well as to share ideas and knowledge globally. It provides essential tools for participation and deliberation in political and other activities of public interest"[13]. The Internet, is undoubtedly global, and based on a distributed and decentralized open and non-proprietary architecture system with invisible national boundaries. The decentralized and borderless nature of the Internet makes it fundamentally different from other communication technologies.

According to Recommendation CM/Rec(2011)8 of the Committee of Ministers, "the individual's freedom to have access to information and to form and express opinions, and the ability of groups to communicate and share views on the Internet depend on actions related to the Internet's

[11] See Bendrath, R., Mueller, M., 'The end of the net as we know it: Deep Packet Inspection and Internet Governance', available at <papers.ssrn.com/sol3/papers.cfm?abstract_id=1653259&download=yes>. According to this report, DPI allows network operators to scan the address and the content of IP packets and in turn classify and control traffic based on the content, applications, and subscribers. DPI equipment is used to manage bandwidth, to carry out real-time government surveillance of Internet communications, to identify and block access to content deemed illegal or harmful, including detection and blocking unauthorised sharing of content protected by copyright.

[12] Adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies.

[13] Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet, adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies (para 3).

infrastructure and critical resources, and on decisions on information technology design and deployment[14]".

Freedom of Expression and the Internet

According to the European Court of Human Rights the Internet is "an information and communication tool particularly distinct from the printed media, in particular as regards the capacity to store and transmit information. The electronic network serving billions of users worldwide is not and potentially cannot be subject to the same regulations and control. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, … is certainly higher than that posed by the press."[15] Furthermore, according to the Court "in light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally."[16] The Court, in *Ahmet Yildirim v. Turkey*, went further by stating that the Internet "had now become one of the principal means of exercising the right to freedom of expression and information."[17]

In line with international human rights instruments including the European Convention on Human Rights, the right to freedom of expression, amongst others, contains not only to impart but also to seek and receive information. Article 10 of the European Convention on Human Rights applies not only to the content of information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information[18]. Furthermore, freedom to receive information is not limited to the forum state. On the contrary, as stated in Article 10 of the Convention and recognised by the European Court freedom to receive information applies "regardless of frontiers"[19]. More importantly, the State must not stand between the speaker and his audience and thus
defeat the purpose for which the protection of expression is realised[20].

Strict Criteria under Article 10 of the European Convention on Human Rights

The European Court has made clear that "freedom of political debate is at the very core of the concept of a democratic society which prevails throughout the Convention"[21]. Under Article 1 of the European Convention, each Contracting State "shall secure to everyone within [its] jurisdiction the rights and freedoms defined in ... [the] Convention"[22].

Within the Council of Europe region, any restriction regarding Internet speech and content must meet the strict criteria under Article 10 of the European Convention on Human Rights.

---

[14] protection and promotion of the universality, integrity and openness of the Internet, adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies (para 4).

[15] See Editorial Board of Pravoye Delo and Shtekel v. Ukraine, Application no. 33014/05, Judgment of 05.05.2011, para 63.

[16] See *Times Newspapers Ltd (Nos. 1 and 2) v. The United Kingdom*, Applications 3002/03 and 23676/03, Judgment of 10 March 009, Final: 10 June 2009; and *Ashby Donald and Others v. France*, no. 36769/08, § 34, 10 January 2013 –not yet final

[17] Ahmet Yildirim v. Turkey, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013 (final).

[18] Autronic AG v. Switzerland, 22 May 1990, §§ 47-48, Series A no. 178; Öztürk v. Turkey [GC], no. 22479/93, § 49, ECHR 1999-VI.

[19] Case of Groppera Radio Ag And Others v. Switzerland, Application no. 10890/84, judgment of 28/03/1990, para. 50.

[20] Ibid.

[21] Lingens v. Austria, Series A no. 103, 8.7.1986, para. 42.

[22] Marckx v. Belgium 13 June 1979, § 31, Series A no. 31; see also Young, James and Webster v. the United Kingdom, 13 August 1981, § 49, Series A no. 44.

According to the European Court of Human Rights jurisprudence, a strict three-part test is required for any content-based restriction. The Court notes that the first and most important requirement of Article 10 of the Convention is that any interference by a public authority with the exercise of the freedom of expression should be lawful.

Article 10 of the Convention stipulates that:

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.[23]

The second paragraph of Article 10 clearly stipulates that any restriction on expression must be "prescribed by law". In order to comply with this important requirement, interference does not merely need a basis in domestic law. The law itself must correspond to certain requirements of "quality". In particular, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct[24]. The degree of precision depends, to a considerable extent, on the content of the instrument at issue, the field it is designed to cover, and the number and status of those to whom it is addressed.[25] The notion of foreseeability applies not only to a course of conduct, but also to "formalities, conditions, restrictions or penalties," which may be attached to such conduct, if found to be in breach of the national laws.[26] If the interference is in accordance with law, then the aim of the restriction should be legitimate based on the Article 10(2) limitations in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others. Finally, the restrictions need to be necessary in a democratic society[27], and the state interference should correspond to a "pressing social need"[28]. The state response and the limitations provided by law should be "proportionate to the legitimate aim pursued"[29]. The European

[23] Note also Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights within this context. See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Human Rights Committee, Geneva, 11-29 July 2011, at http://www2.ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34.doc. See further General Comment No.34 on Article 19 which was adopted during the 102nd session of the UN Human Rights Committee, Geneva, 11-29 July 2011, at <http://www2.ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34.doc>.

[24] See, for example, Lindon, Otchakovsky-Laurens and July v. France [GC], nos. 21279/02 and 36448/02, § 41, ECHR 2007-XI.

[25] See *Kafkaris v. Cyprus* [GC], no. 21906/04, § 140, ECHR 2008.

[26] See Sunday Times v. UK (No. 2), Series A No. 217, 26.11.1991, para. 50; Okçuoglu v. Turkey, No. 24246/94, 8.7.1999, para. 43.

[27] See *Sürek v. Turkey* (No. 1) (Application No. 26682/95), judgment of 8 July 1999, Reports 1999; Sürek (No. 3) judgment of 8 July 1999.

[28] See Bladet Tromsø and Stensaas v. Norway [GC], no. 21980/93, ECHR 1999-III.

[29] The Court notes that the nature and severity of the penalty imposed, as well as the "relevance" and "sufficiency" of the national courts' reasoning, are matters of particular significance when it comes to assessing the proportionality of an interference under Article 10(2): See *Cumpana and Mazare v. Romania* [GC], no. 33348/96, § 111, ECHR 2004, and *Zana v. Turkey*, 25 November 1997, § 51, Reports of Judgments and Decisions 1997-VII. The Court also reiterates that Governments should always display restraint in resorting to criminal sanctions, particularly where there are other means of redress available. See further *Baskaya and Okçuoglu* judgment of 8 July 1999, Reports 1999.

Court of Human Rights requires the reasons given by the national authorities to be relevant and sufficient[30].

Contracting States of the Council of Europe have a certain margin of appreciation in assessing whether a "pressing social need" exists to introduce speech-based restrictions to their national laws based on Article 10 of the European Convention on Human Rights. Nevertheless, the state action is subject to European supervision through the European Court of Human Rights, and the necessity of the content-based restrictions must be convincingly established by the contracting states[31]. The Court is therefore empowered to give the final ruling on whether a "restriction" is reconcilable with freedom of expression as protected by Article 10[32]. The Court's supervision will be strict because of the importance given to freedom of expression. While the measure taken need not be shown to be "indispensable", the necessity for restricting the right must be convincingly established[33]. According to the Council of Europe Committee of Experts for the Development of Human Rights (DH-DEV) "at the core of the examination of any interference in the exercise of freedom of opinion is therefore a balancing of interests, in which the Court takes account of the significance of freedom of opinion for democracy"[34].

The Article 10 compatibility criteria as set out by the European Court of Human Rights should be taken into account while developing content related policies and legal measures by the participating States.

Cross Border Impact of State Policies and Actions

In November 2007, Committee of Ministers Recommendation on measures to promote the public service value of the Internet[35] called upon the Member States to promote freedom of communication and creation on the Internet regardless of frontiers, in particular by not subjecting individuals to any licensing or other requirements having a similar effect, nor any general blocking or filtering measures by public authorities, or restrictions that go further than those applied to other means of content delivery[36]. In March 2008, the Committee of Ministers in a new Recommendation[37] recalled the Declaration of the Committee of Ministers on freedom of communication on the Internet of May 2003[38] which stressed that public authorities should not, through general blocking or filtering measures, deny access to the public information and other communication on the Internet regardless of frontiers[39]. The Committee of Ministers in its March 2008 Recommendation stated that "there is a tendency to block access to the population to content on certain foreign or domestic web sites for political reasons. This and similar practices of prior State control should be strongly condemned."

---

[30] *The Observer and The Guardian v. the United Kingdom*, judgment of 26 November 1991, Series A no. 216, pp. 29-30, § 59.

[31] *Lingens v. Austria*, 8 July 1986, Series A No. 103, p. 26, § 41; Perna v. Italy [GC], no. 48898/99, § 39, ECHR 2003-V; and *Association Ekin v. France*, no. 39288/98, § 56, ECHR 2001-VIII.

[32] Autronic AG judgment of 22 May 1990, Series A No. 178, § 61.

[33] Council of Europe Steering Committee For Human Rights (CDDH), Committee of Experts for the Development of Human Rights (DH-DEV), Working Group A, Report on "Hate Speech", document GT-DH-DEV A(2006)008, Strasbourg, 9 February 2007, para. 22. Note further the Handyside judgment of 7 December 1976, Series A No. 24, §49.

[34] CM/Rec(2007)16 of November, 2007.

[35] Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet: Adopted by the Committee of Ministers on 7 November, 2007 at the 1010th meeting of the Ministers' Deputies

[36] Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters: Adopted by the Committee of Ministers on 26 March, 2008 at the 1022nd meeting of the Ministers' Deputies.

[37] Freedom of communication on the Internet, Declaration adopted by the Council of Europe Committee of Ministers on 28 May, 2003 at the 840th meeting of the Ministers' Deputies.

[38] Ibid, Principle 3.

[39] SSAC Advisory on Impacts of Content Blocking via the Domain Name System, SAC056, 09 October 2012.

Furthermore, CoE Recommendation of March 2008 stated that any intervention by Member States that forbids access to specific Internet content may constitute a restriction on freedom of expression and access to information in the online environment and that such a restriction would have to fulfil the conditions in Article 10(2) of the European Convention on Human Rights and the relevant case law of the European Court of Human Rights. The Recommendation noted that the voluntary and responsible use of Internet filters (products, systems and measures to block or filter Internet content) can promote confidence and security on the Internet for users, in particular for children and young people, while also noting that the use of such filters can seriously impact on the right to freedom of expression and information as protected by Article 10 of the ECHR. The Guidelines called upon the Member States to refrain from filtering Internet content in electronic communications networks operated by public actors for reasons other than those laid down in Article 10(2) of the ECHR as interpreted by the European Court of Human Rights.

According to the Guidelines such action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body in accordance with the requirements of Article 6 of the ECHR. The Guidelines also called upon the Member States to ensure that all filters are assessed both before and during their implementation to ensure that the effects of the filtering are proportionate to the purpose of the restriction and thus necessary in a democratic society, in order to avoid unreasonable blocking of content.

Possible Scenarios Involving the Cross Border Impact of State Policies with regard to Restrictions on Internet Content

Possible scenarios involving the cross border impact of state policies with regards to restrictions on Internet content will be analysed below.

Scenario I: Impact of DNS/IP Blocking and Filtering Policies on Freedom of Expression

Legal provisions as well as voluntary mechanisms and agreements for blocking access to certain types of Internet content exist in a number of Council of Europe Member States. Certain states also adopted filtering policies and upstream filtering systems are used by a number of Internet Service Providers within the Council of Europe region. However, state-level legal or non-legal blocking and filtering policies could undoubtedly have a serious impact on freedom of expression, which is one of the founding principles of democracy.

ICANN Security and Stability Advisory Committee (SSAC) stated that "overall Internet stability require that any DNS blocking policy or action be fully disclosed to affected parties including end users, service providers, and application designers. DNS blocking in the absence of such disclosure will lead to unnecessary troubleshooting activities as well as adaptive and perhaps even unintended bypass activities by network operators and end users."[40]

If a Member State adopts a DNS and/or IP based blocking/tampering policy this may have certain implications and significant side effects that will be assessed below.

A. Over-blocking within the State

If a Member State adopts a DNS and/or IP based blocking/tampering policy this may lead into over-blocking within that particular state. As explained by the ICANN Security and Stability Advisory Committee (SSAC)

> "it is important to recognize that if blocking is implemented for a domain such as example.com, blocking using the domain name system will not only block the ability to look up the domain name when accessing content under the blocked URL http://example.com/bad-content.html, but

[40] SSAC Advisory on Impacts of Content Blocking via the Domain Name System, SAC056, 09 October 2012.

also all other URLs using that same domain name; e.g., under http://abc.example.com/ or http://example.com/good-content.html. DNS blocking will also block domain name lookup for all other services such as e-mail, network management, file transfer, etc. that use the same domain, and additionally, child domains of example.com (e.g., subdomain.example.com)."[41]

This scenario can take place when the execution of a blocking order involves an Internet portal or a social media platform such as YouTube, Twitter, or Facebook rather than a single static website. Rather than blocking access to a single page or a series of pages and content deemed allegedly illegal by state authorities or local courts, the DNS and/or IP based blocking results in blocking access to all the content
provided on that particular web based portal or platform.

Such a scenario was the subject matter of an application to the European Court of Human Rights. *Ahmet Yildirim v. Turkey*[42] involved a court decision to block access to Google Sites, which hosted an Internet site whose owner was facing criminal proceedings for insulting the memory of Atatürk. As a result of the court decision, access to all other sites hosted by Google Sites was also blocked including the applicant's websites hosted on Google Sites. The responsible public authority made it technically impossible to access any content on Google Sites in order to implement the measure ordered by the local court. The measure in question therefore amounted to interference by the public authorities with the applicant's right to freedom of expression. Such interference would breach Article 10 unless it was prescribed by law, pursued one or more legitimate aims and was necessary in a democratic society to achieve such aims.

In its first access blocking related decision, the European Court of Human Rights, finding a violation of Article 10 of the European Convention on Human Rights, held that a restriction on access to a source of information is only compatible with the Convention if a strict legal framework is in place regulating the scope of a ban and affording the guarantee of judicial review to prevent possible abuses.

The Court further observed that there was no indication that the Criminal Court had made any attempt to weigh up the various interests at stake, in particular by assessing whether it had been necessary to block all access to Google Sites. In the Court's view, this shortcoming was a consequence of the domestic law, which did not lay down any obligation for the courts to examine whether the wholesale blocking of Google Sites was justified. The courts should have had regard to the fact that such a measure would render large amounts of information inaccessible, thus directly affecting the rights of Internet users and having a significant collateral effect.

The Court also pointed out that Article 10(1) of the Convention stated that the right to freedom of expression applied "regardless of frontiers". The effects of the measure in question had therefore been arbitrary and the judicial review of the blocking of access had been insufficient to prevent abuses.

Therefore, even provided that a legal basis exists for blocking access to websites, any interference must be proportionate to the legitimate objective pursued. Within this context, following *Ahmet Yildirim v. Turkey*[43] blocking access to web portals and social media platforms is incompatible with Article 10 of the European Convention on Human Rights, and could be regarded as a serious infringement on freedom of expression. Such a disproportionate and broad measure would be more far reaching than reasonably necessary in a democratic society.[44]

---

[41] SSAC Advisory on Impacts of Content Blocking via the Domain Name System, SAC056, 09 October 2012 at http://www.icann.org/en/groups/ssac/documents/sac-056-en.pdf

[42] *Ahmet Yildirim v. Turkey*, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013

[43] Ahmet Yildirim v. Turkey, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013 (final).

[44] *Khurshid Mustafa and Tarzibachi v. Sweden*, App. no. 23883/06, judgment of 16 December 2008.

B. Collateral Damage and Over Blocking within the State

If a Member State adopts a DNS and/or IP based blocking/tampering policy this may lead into causing collateral damage and unintended consequences within that particular state. There is particular concern that especially with IP blocking policies state authorities may also block access to legitimate content that is not the intended consequence of a blocking order or decision.

By way of example, in May 2008, an injunction to block access to the Google owned popular video-sharing web 2.0 platform YouTube was issued by a court in Turkey[45].

The Court order intended to block access to allegedly illegal 10 video files available through the YouTube platform. Access to the YouTube website has been constantly blocked from Turkey until 30 October 2010. During the blocking period, the Court also issued a supplemental blocking order during June 2010[46]. This supplemental decision was issued subsequent to the demands of the Ankara Chief Public Prosecutor's Office to block access to 44 additional IP addresses related to the YouTube website[47]. According to the Court, this supplemental decision was deemed necessary as the YouTube website was providing access through various domain names across several DNS servers abroad by routing IP addresses which are dynamically changing. The Court stated that if such different DNS servers are used then the website, can be accessed from Turkey despite the initial injunction of May 2008. However, blocking access to 44 IP addresses used by Google resulted with disrupting, interrupting and in some instances completely blocking the below named Google owned services and websites which were not part of the court issued blocking order:

http://code.google.com http://pages.google.com http://video.google.com
http://translate.google.com.tr http://docs.google.com http://books.google.com
http://chrome.google.com http://sketchup.google.com http://froogle.google.com
http://labs.google.com http://mars.google.com http://moon.google.com
http://notebook.google.com http://toolbar.google.com http://browsersync.google.com
http://catalog.google.com http://codesearch.google.com http://dir.google.com
http://earth.google.com http://groups.google.com.tr http://shopping.google.com
http://sky.google.com http://support.google.com http://tools.google.com
http://wap.google.com http://answers.google.com http://google-analytics.com
http://maps.google.com/ http://picasa.google.com/ http://www.google.com/chrome

In other words, although there has been no blocking order that has been issued for these sites, access ban has been indirectly applied on these popular websites and services from Turkey.

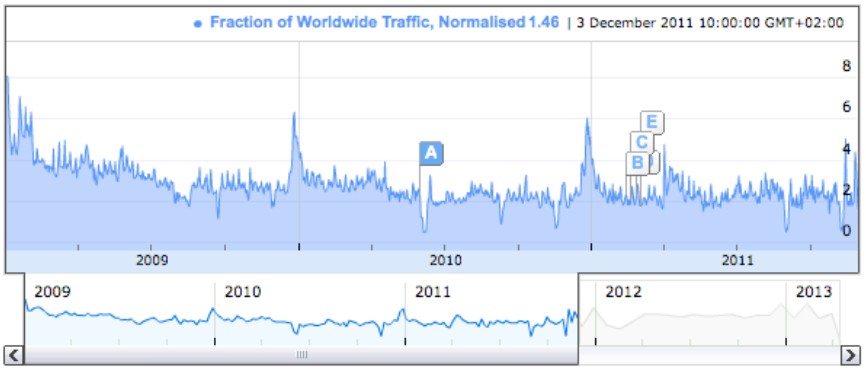
[45] Ankara 1st Criminal Court of Peace, decision no 2008/402, date 05.05.2008. The court order requested blocking access to the domain of www.youtube.com and certain related IP addresses (208.65.153.238-208.65.153.251 and 208.65.153.253).

[46] Ankara 1st Criminal Court of Peace, supplemental decision no 2008/402 Misc., date 17.06.2010.

[47] The IP numbers named on the supplemental decision of the Ankara 1st Criminal Court of Peace are: 74.125.47.136-74.125.47.93-74.125.47.190-74.125.47.91-209.85.227.190-209.85.227.91209-85.229.93-209.85.229.136-209.85.229.190 74.125.43.93-74.125.43.190-74.125.43.19174.125.43.136-74.125.39.93-74.125.39.91-74.125.39.190-74.125.39.136-74.125.79.9174.125.79.190-74.125.79.136-74.125.127.190-74.125.127.91-74.125.127.93-74.125.93.13674.125.93.190-74.125.93.91-74.125.93.93-74.125.95.136-74.125.95.190 - 74.125.93.190.74.125.95.91 and 74.125.95.93

Turkey | Google Docs

Fraction of Worldwide Traffic, Normalised



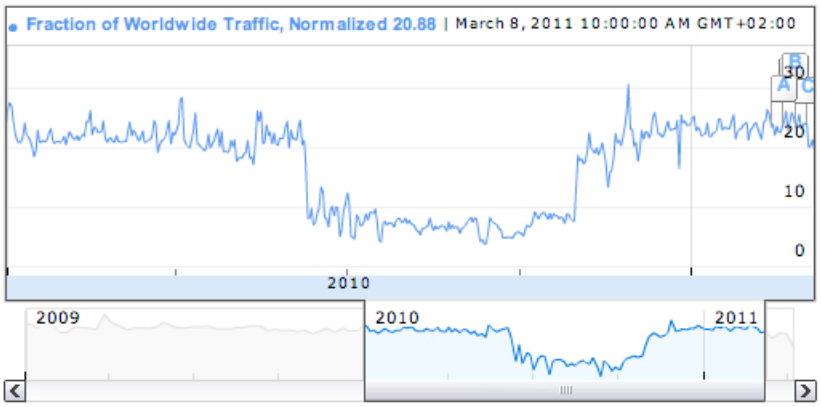
C. We changed how we classify some traffic.
2011-2-18

B. We changed how we classify some traffic.
2011-2-12

A. Adwords, Analytics and Docs inaccessible for a week during an attempt to block YouTube. [Source: ONI]
2010-5-31

Turkey | Google Earth

Google Earth, Turkey Traffic Divided by Worldwide Traffic and Normalized



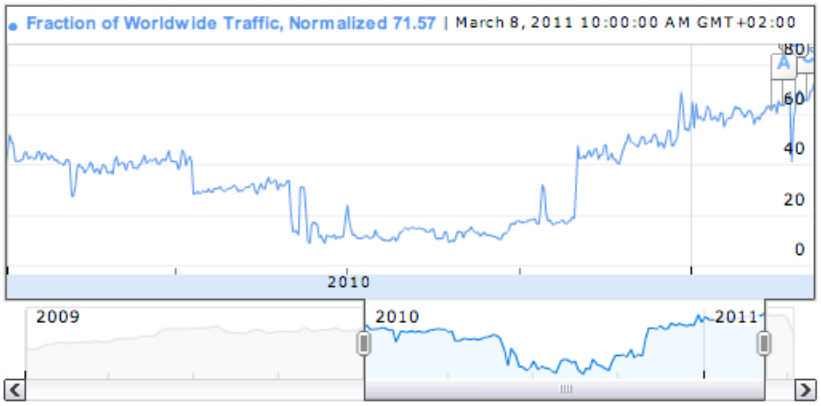
E. Apr 8, 2
this poi
finalize
with ca
2011-4-9

D. Mar 3, 2
change
some tr
2011-3-3

C. Feb 25,
change
some tr

Turkey | YouTube

YouTube, Turkey Traffic Divided by Worldwide Traffic and Normalized



E. Apr 8, 2
this poi
finalize
with ca
2011-4-9

D. Mar 3, 2
change
some tr
2011-3-3

C. Feb 25,
change
some tr

In a similar incidence, when a court in Kazakhstan ordered to block access to www.geo.kz and its related mirror sites including one on LiveJournal, access to the whole of the LiveJournal social media platform was blocked from Kazakhstan in May 2009.[48] Access to the LiveJournal was also completely blocked from Russia, albeit temporarily to the city of Yaroslavl and part of surrounding Moscow from July 18 to 20, 2012[49]. A Yaroslavl court ordered Internet provider Netis Telekom to block access to a neo-Nazi blog hosted on the LiveJournal social media platform and requested the ISP to block access to a certain IP address (208.93.0.128). This resulted with blocking access to the whole site. Similarly, in July 2010, the Russian "Rosnet" was compelled to limit users' access to YouTube, as the platform hosted "Russia For Russians", an ultra-nationalist video on the Russian Justice Ministry's federal list of banned extremist materials. The court ban extended to four other electronic libraries (Web.archives.org, Lib.rus.ec, Thelib.ru and Zhurnal.ru) after experts found extremist materials on these websites, including the text of Adolf Hitler's 'Mein Kampf', also placed on the federal list of extremist materials banned for distribution in the Russian Federation[50].

Therefore, DNS blocking and IP address blocking methods currently used in some countries may result in massive over-blocking that is beyond the intended aim pursued by the state authorities. Having regard to the principle that the Convention and its Protocols must be interpreted in the light of present-day conditions[51] and following the decision of the European Court of Human Rights in *Ahmet Yildirim v. Turkey*,[52] adoption of such a broad blocking policy or the application of a broadly worded court issued blocking order would certainly be in breach of Article 10 and would be regarded as disproportionate as the exceptions to Article 10 of the European Convention on Human Rights must be narrowly interpreted and the necessity for any restrictions must be convincingly established.

C. Cross Border Impact of State Blocking and Filtering Policies

If a Member State adopts a DNS and/or IP based blocking policy or an upstream filtering policy this may lead into causing collateral damage and unintended consequences in another state if Internet access is provided by an Internet Service Provider (state owned or private) based in the state (State A) implementing blocking or filtering policy to another neighbouring state (State B). By way of example, the
OpenNet Initiative found out in 2009 that a number of websites, including news sites and blogging platforms, were inaccessible in Kyrgyzstan "as a result of blocking by the state ISP in Kazakhstan, which sells its service to KyrgyzTelecom"[53]. The OpenNet Initiative observed similar behaviour in Uzbekistan in 2004 "where content filtering on one Uzbek ISP closely matched that seen in China, a finding supplemented by evidence that this ISP was purchasing connectivity service from China Telecom."[54] More recently, The Citizen Lab at the University of Toronto published research that showed that "web filtering applied by India-based ISPs is restricting access to content for customers of an ISP in Oman."[55] The Citizen Lab report stated that "while unusual, content filtering undertaken in one

[48] See Ekspress-K newspaper, No. 337 (16723) of 26 May 2009.

[49] See further http://www.dailydot.com/news/russian-livejournal-censorship-8941760-blacklist/

[50] See The Guardian, "YouTube banned by Russian court," 29 July 2010, at <http://www.guardian.co.uk/world/2010/jul/29/youtube-ban-russian-regional-court>.

[51] See *Tyrer v. the United Kingdom*, 25 April 1978, § 31, Series A no. 26, and *Vo v. France* [GC], no. 53924/00, § 82, ECHR 2004-VIII.

[52] *Ahmet Yildirim v. Turkey*, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013 (final).

[53] See OpenNet Initiative, "Kyrgyzstan," (2010) at http://opennet.net/sites/opennet.net/files/ONI_Kyrgyzstan_2010.pdf

[54] See OpenNet Initiative, "Internet filtering in the Commonwealth of Independent States 20062007"

(updated in 2010) at http://opennet.net/sites/opennet.net/files/ONI_CIS_2010.pdf

[55] See The Citizen Lab, University of Toronto, "Routing Gone Wild: Documenting upstream filtering in Oman via India," 12 July, 2012, at https://citizenlab.org/wpcontent/uploads/2012/07/08-2012-routinggonewild.pdf

political jurisdiction can have an effect on users in another political jurisdiction as a result of ISP routing arrangements – a phenomenon known as 'upstream filtering.'"[56]

The important question that would arise in this scenario is whether the Contracting States of the Council of Europe would be responsible for breaches of the European Convention on Human Rights if their state level blocking or filtering policies have cross border implications in another neighbouring state. In a hypothetical case the question would be whether an applicant based in State B can complain of acts (in this scenario blocking access to websites) which can be attributed to State A even though the acts were not performed on the territory of State B.

So far as jurisdiction issues are concerned Article 1 of the European Convention on Human Rights states that:

> "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of [the] Convention."

It follows from Article 1 that Member States must answer for any infringement of the rights and freedoms protected by the Convention committed against individuals placed under their "jurisdiction"[57]. According to the European Court of Human Rights "the exercise of jurisdiction is a necessary condition for a Contracting State to be able to be held responsible for acts or omissions imputable to it which give rise to an allegation of the infringement of rights and freedoms set forth in the Convention."[58] Therefore, a Contracting Party "is responsible under Article 1 of the Convention for all acts and omissions of its organs regardless of whether the act or omission in question was a consequence of domestic law or of the necessity to comply with international legal obligations."[59] Furthermore, "Article 1 makes no distinction as to the type of rule or measure concerned and does not exclude any part of a Contracting Party's "jurisdiction" from scrutiny under the Convention."[60]

The European Court refers to its case-law to the effect that the concept of "jurisdiction" for the purposes of Article 1 of the Convention must be considered to reflect the term's meaning in public international law.[61] From the standpoint of public international law, the words "within their jurisdiction" in Article 1 of the Convention must be understood to mean that a State's jurisdictional competence is primarily territorial.[62] The Court has found clear confirmation of this essentially territorial notion of jurisdiction in the travaux préparatoires[63], given that the Expert Intergovernmental Committee

---

[56] Ibid.

[57] It should be emphasised that "The Court's case-law on Article 1 of the Convention (the jurisdiction of the Contracting Parties) has, so far, been bedevilled by an inability or an unwillingness to establish a coherent and axiomatic regime, grounded in essential basics and even-handedly applicable across the widest spectrum of jurisdictional controversies." Per Judge Bonello, concurring opinion in *Al Skeini and Others v. The United Kingdom*, Application no. 55721/07, 7 July 2011, para 4.

[58] See *Ilascu and Others v. Moldova and Russia*, [GC], no. 48787/99, § 311, ECHR 2004*; Issa and Others v. Turkey*, Application no. 31821/96, Judgment of 16 November 2004 (Final: 30.03.2005).

[59] See Al-Saadoon and Mufdhi v. the United Kingdom (no. 61498/08), para 128.

[60] *Al-Saadoon and Mufdhi v. the United Kingdom* (no. 61498/08), para 128. See further Case of *Bosphorous Hava Yollari Turizm ve Ticaret Anonim Sirketi v. Ireland* (Application No. 45036/98), Judgment of 30 June 2005; *United Communist Party of Turkey and Others v. Turkey*, judgment of 30 January 1998, Reports 1998-I, pp. 17-18, § 29.

[61] See *Gentilhomme and Others v. France*, nos. 48205/99, 48207/99 and 48209/99, § 20, judgment of 14 May 2002*; Bankovic and Others v. Belgium and Others* (dec.) [GC], no. 52207/99, §§ 5961, ECHR 2001-XII; and *Assanidze v. Georgia* [GC], no. 71503/01, § 137, ECHR 2004-II.

[62] See Bankovic and Others v. Belgium and Others (dec.) [GC], no. 52207/99, §§ 59-61, ECHR 2001-XII.

[63] See further Collected Edition of the Travaux Préparatoires of the European Convention on Human Rights (Vol. III, p. 260) which states that "The Assembly draft had extended the benefits of the Convention to 'all persons residing within the territories of the signatory States'. It seemed to the Committee that the term 'residing' might be considered too restrictive. It was felt that there were good grounds for extending the benefits of the Convention to all persons in the territories of the signatory States, even those who

replaced the words "all persons residing within their territories" with a reference to persons "within their jurisdiction" with a view to expanding the Convention's application to others who may not reside, in a legal sense, but who are, nevertheless, on the territory of the Contracting States.

However, the concept of "jurisdiction" is not necessarily restricted to the national territory of the High Contracting Parties[64]. The European Court of Human Rights has accepted that in exceptional circumstances the acts of Contracting States performed outside their territory, or which produce effects there ("extraterritorial acts"), may amount to exercise by them of their jurisdiction within the meaning of Article 1 of the Convention.[65] The European Court in its case-law has recognised a number of exceptional circumstances capable of giving rise to the exercise of jurisdiction by a Contracting State outside its own territorial boundaries.[66] According to the Court, "in each case, the question whether exceptional circumstances exist which require and justify a finding by the Court that the State was exercising jurisdiction extraterritorially must be determined with reference to the particular facts."[67] In sum, the case-law of the Court demonstrates that its recognition of the exercise of extraterritorial jurisdiction by a Contracting State is exceptional: it has done so when the respondent State, through the effective control of the relevant territory and its inhabitants abroad as a consequence of military occupation or through the consent, invitation or acquiescence of the Government of that territory, exercises all or some of the public powers normally to be exercised by that Government.[68]

Although a "cause-and-effect" type of State responsibility has not been adopted by the European Court of Human Rights, it remains to be seen whether the Court would interpret Internet access blocking as an extra-territorial act if a state owned or private Internet Service Provider based in a Contracting State (State A) provides Internet access to another Contracting State (State B). In such a scenario the European Court would assess the connection between the applicant from State B and the respondent State A and whether the impugned act (access blocking) had effects outside the territory of State A ("the extra-territorial act"). The notion of the Convention being a living instrument to be interpreted in the light of present day conditions is firmly rooted in the Court's case-law[69] and "that the increasingly high standard being required in the area of the protection of human rights and fundamental liberties correspondingly and inevitably requires greater firmness in assessing breaches of the fundamental values of democratic societies."[70] Furthermore, in *Al Skeini and Others v. The United Kingdom*, the European Court, leaving open the debate on State liability, held that that it does not mean that "jurisdiction under Article 1 of the Convention can never exist outside the territory covered by the Council of Europe Member States."[71]

Therefore, in such a hypothetical scenario, Internet access blocking could be regarded as an "exceptional case" by the European Court even though the impugned act takes place outside its

---

could not be considered as residing there in the legal sense of the word. The Committee therefore replaced the term 'residing' by the words 'within their jurisdiction' which are also contained in Article 2 of the Draft Covenant of the United Nations Commission."

[64] See Loizidou v. Turkey judgment of 18 December 1996, Reports of Judgments and Decisions 1996-VI, pp. 2235-2236 § 52.

[65] See among others see Drozd and Janousek v. France and Spain, judgment of 26 June 1992, Series A no. 240, § 91; Loizidou v. Turkey (preliminary objections), 23 March 1995, § 62, Series A no. 310; Loizidou v. Turkey (merits), 18 December 1996, § 52, Reports of Judgments and Decisions 1996-VI. The statement of principle, as it appears in Drod and Janousek and the other cases is very broad: the Court states merely that the Contracting Party's responsibility "can be involved" in these circumstances (Al Skeini and Others v. The United Kingdom, Application no. 55721/07, 7 July 2011, para 133). Note also Mohammed Ben El Mahi and Others v. Denmark (App. No. 5853/06), 11 December 2006 (admissibility decision).

[66] *Al Skeini and Others v. The United Kingdom*, Application no. 55721/07, 7 July 2011, para 132.

[67] Ibid.

[68] Ibid.

[69] See, for example, Tyrer v. the United Kingdom, 25 April 1978, § 31, Series A no. 26; Airey v. Ireland, 9 October 1979, § 26, Series A no. 32; Vo v. France [GC], no. 53924/00, § 82, ECHR 2004-VIII; and Mamatkulov and Askarov v. Turkey [GC], nos. 46827/99 and 46951/99, § 121, ECHR 2005-I.

[70] Öcalan v. Turkey, App. no. 46221/99, ECHR 2005-IV, (judgement of 12 March 2003), para 193.

[71] See Al Skeini and Others v. The United Kingdom, Application no. 55721/07, 7 July 2011, para 142. See further

territorial jurisdiction. The author of this report agrees with Altiparmak that the problem of jurisdiction should be regarded as one of control rather than effective or overall control. Therefore, the question to be asked is "who does and (who) can control the conduct that harms the rights and freedoms defined in the ECHR?"[72] Judge Bonello in *Al Skeini and Others v. The United Kingdom* stated that "jurisdiction means no less and no more than "authority over" and "control of"" and "jurisdiction is neither territorial nor extra-territorial: it ought to be functional"[73] in relation to Convention obligations. Therefore, in our hypothetical scenario the answer would be the state implementing access blocking policy would be in control, with detrimental cross border impact of that policy in a neighbouring state.

Furthermore, this idea could find strong support from the recent decision of the European Court of Human Rights in *Ahmet Yildirim v. Turkey*[74]. The Court in Yildirim addressed the issue of access blocking policies and their detrimental side effects finding an infringement of Article 10. Although there were no cross border effects of the blocking order issued by the local court in Turkey, the European Court stated that "Article 10 guaranteed freedom of expression to "everyone" and applied not only to the content of information but also to the means of disseminating it" regardless of frontiers.[75]

Scenario II: Impact of State Kill Switch Policies

It is worth mentioning that certain States may implement kill switch policies to completely cut off to Internet services in certain circumstances. Such policies exist in certain States to be used during times of war, states of emergency and in cases of imminent threat to national security. By way of example, in Azerbaijan, Clause 3 of the "Order of the Azerbaijan Republic Ministry of Communications and Information Technologies" issued on 24 February 2000, states that a provider can suspend delivery of Internet services in certain circumstances, including in times of war or state of emergency, natural disasters, or other catastrophes or when services are provided to third parties without the appropriate license, and in cases where systems that are either defective or uncertified are connected to the network. Delivery of Internet services can also be suspended in cases that run against the rules established by the legislation of the Azerbaijan Republic and the law "on Telecommunications".

A recent example of this policy trend and action was witnessed in Syria on 07 May 2013 when Syria has largely disappeared from the Internet.[76] The blackout lasted 19 hours and 27 minutes. It is strongly suggested that the Syrian government is responsible for the blackout rather than damage to critical Internet infrastructure.

[72] See Altiparmak, K., "Bankovic: An Obstacle to the Application of the European Convention of Human Rights in Iraq?" Journal of Conflict & Security Law (2004), Vol. 9 No. 2, 213–251, at p. 241.

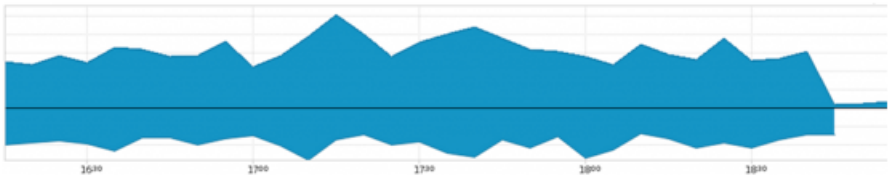
[73] Per Judge Bonello, concurring opinion in Al Skeini and Others v. The United Kingdom, Application no. 55721/07, 7 July 2011, para 12.

[74] *Ahmet Yildirim v. Turkey*, Application no.3111/10, judgment of 18 December 2012, 18.03.2013 (final).

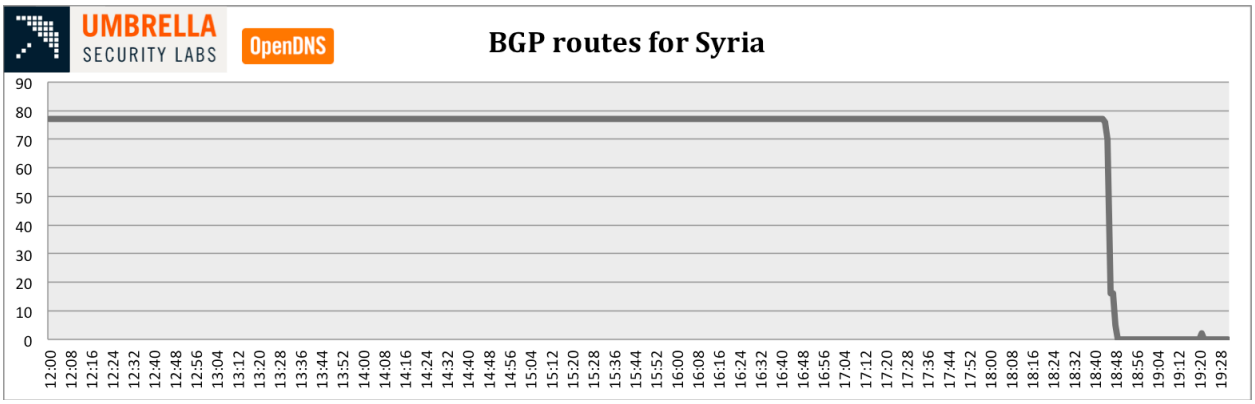
[75] Ibid.

[76] See generally Umbrella Security Labs, "Breaking news: Traffic from Syria Disappears from Internet," 07 May 2013 at http://labs.umbrella.com/2013/05/07/breaking-news-traffic-from-syriadisappears-from-internet/

The graph below shows DNS traffic from and to Syria. The drop in both inbound and outbound traffic from Syria is clearly visible. The small amount of outbound traffic depicted by the chart indicates our DNS servers trying to reach DNS servers in Syria.



According to Umbrella Security Labs, "there have been numerous incidents where access to and from the Internet in Syria was shut down. Shutting down Internet access to and from Syria is achieved by withdrawing the BGP routes from Syrian prefixes. The graph below shows the sudden drop in visibility for Syrian network prefixes."



A Kill Switch Policy could have detrimental effects not only within the state implementing such a policy but also have detrimental cross border effects in a neighbouring state if the neighbouring state obtains Internet access from the state implementing a Kill Switch Policy. In a hypothetical case the question would be whether an applicant based in State B can complain of acts (in this scenario Kill Switch Policy) which can be attributed to State A even though the acts were not performed on the territory of State B. As established above responsibility for breaches of the European Convention on Human Rights could arise for the Contracting States of the Council of Europe but this would depend upon whether the European Court would interpret complete cutting off Internet services in certain circumstances, albeit for a limited period of time as an extra-territorial act in another state and within the responsibility of the state providing Internet access services.

Conclusion and Recommendations

According to the European Court, the Internet has now become one of the main ways people exercise their right to freedom of expression and information. Under the European Convention on Human Rights the Contracting States have the obligation to secure to everyone under their jurisdiction the protection of the right to freedom of expression, including the freedom to hold opinions and to receive and impart information and ideas without interference by public authorities subject to Article 10 of the European Convention of Human Rights. Furthermore, freedom to receive information is not limited to the forum state. On the contrary, as stated in Article 10 of the Convention and recognised by the European Court of Human Rights freedom to receive information applies "regardless of frontiers".[77]

Positive Obligation to Protect Freedom of Expression

The European Court has held that although the essential object of many provisions of the Convention is to protect the individual against arbitrary interference by public authorities, there may in addition be positive obligations inherent in effect respect of the rights concerned. A positive obligation may also arise under Article 10.[78] The European Court emphasized the key importance of freedom of expression as one of the preconditions for a functioning democracy in a number of its decisions and established that genuine, effective exercise of this freedom does not depend merely on the State's duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals.[79]

In determining whether or not a positive obligation exists, regard must be had to the fair balance that has to be struck between the general interest of the community and the interests of the individual, the search for which is inherent throughout the Convention. The scope of this obligation will inevitably vary, having regard to the diversity of situations obtaining in Contracting States and the choices which must be made in terms of priorities and resources. Nor must such an obligation be interpreted in such a way as to impose an impossible or disproportionate burden on the authorities.[80]

Based on the positive obligation to protect principle developed by the European Court, it is argued that Contracting States do have a positive obligation to ensure that they do not interfere with the cross border flow of the Internet from their territories to neighbouring states. If a particular Contracting State or an Internet Service Provider based in that Contracting State provides Internet access to a neighbouring state, then the Contracting State is obliged to ensure that restrictions that may be imposed locally should not interfere with the free flow of information and Internet access within the neighbouring state(s). As established in *Ahmet Yildirim v. Turkey*,[81] blocking access to a website would constitute interference with the exercise of the rights guaranteed by Article 10(1) of the European Convention as Article 10 applies not only to the content of the information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information.[82]

---

[77] Case of *Groppera Radio Ag And Others v. Switzerland*, Application no. 10890/84, judgment of 28/03/1990, para. 50.

[78] See generally European Court of Human Rights (Research Division), Positive obligations on member States under Article 10 to protect journalists and prevent impunity, Research Report, December 2011.

[79] See *Özgür Gündem v. Turkey*, no. 23144/93, §§ 42-46, ECHR 2000-III; Fuentes Bobo v. Spain, no. 39293/98, § 38, 29 February 2000.

[80] See, generally *Rees v. the United Kingdom*, judgment of 17 October 1986, Series A no. 106, p. 15, § 37; *Osman v. the United Kingdom*, judgment of 28 October 1998, Reports of Judgments and Decisions 1998-VIII, pp. 3159-60, § 116; *Appleby and Others v. the United Kingdom*, Application no. 44306/98, judgment of 06 May 2003; *Khurshid Mustafa and Tarzibachi v. Sweden*, App. no. 23883/06, judgment of 16 December.

[81] *Ahmet Yildirim v. Turkey*, Application no.3111/10, judgment of 18 December 2012, 18.03.2013 (final).

[82] See further *Öztürk v. Turkey* [GC], no. 22479/93, § 49, ECHR 1999-VI

So far as issues concerning a Contracting State's acts on its own territory producing effect in another State and the relevant jurisprudence of the European Court of Human Rights, it is argued that if a Contracting State "within its authority" controls the conduct that harms the rights and freedoms defined in the European Convention in a neighbouring state by interfering with that state's Internet access, traffic, or access to information then state liability should arise.

Although there is an ongoing debate on the European Court of Human Rights' jurisprudence on Article 1 concerning jurisdiction and what constitutes extraterritorial acts, the European Court's approach to Internet's importance with regards to freedom of expression is clear. According to the Court the Internet has "become one of the principal means of exercising the right to freedom of expression and information."[83] The European Court already addressed the controversial issue of blocking access to websites in its recent decision of *Ahmet Yildirim v. Turkey*[84] and the Court would in the future assess cross border liability in the light of present day conditions[85] requiring high standards in the area of the protection of human rights and fundamental liberties including access to information and freedom of expression.

Based on legal arguments put forward in this report, it appears feasible to develop a Council of Europe instrument designed to reinforce the protection of cross border flow of Internet traffic in line with the CoE Strategy for Internet Governance 2012 2015[86] which identified protecting the Internet's universality, integrity and openness and maximising rights and freedoms for Internet users among its main objectives to advance the protection and respect for human rights, the rule of law and democracy on the Internet.

A recommendation to be adopted by the Committee of Ministers of the Council of Europe should be developed to preserve the protection of cross border flow of Internet traffic to ensure that the Internet is, at all times, accessible without any arbitrary blocking, interference or interruption through the Contracting States.

[83] Ahmet Yildirim v. Turkey, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013 (final).

[84] *Ahmet Yildirim v. Turkey*, Application No. 3111/10, judgment of 18 December 2012, 18.03.2013 (final).

[85] See, for example, *Tyrer v. the United Kingdom*, 25 April 1978, § 31, Series A no. 26; Airey v. Ireland, 9 October 1979, § 26, Series A no. 32; Vo v. France [GC], no. 53924/00, § 82, ECHR 2004-VIII; and *Mamatkulov and Askarov v. Turkey* [GC], nos. 46827/99 and 46951/99, § 121, ECHR 2005-I.

[86] See CM(2011)175 final, 15 March 2012.