Protecting the Core (of the Internet)

Technical Report · November 2017

DOI: 10.13140/RG.2.2.20733.05600

CITATIONS
0

READS
161

3 authors:

Oluwafemi Osho
Federal University of Technology Minna
39 PUBLICATIONS **244** CITATIONS
SEE PROFILE

Joseph Adebayo Ojeniyi
Federal University of Technology Minna
24 PUBLICATIONS **29** CITATIONS
SEE PROFILE

Shafi'i Muhammad Abdulhamid
Federal University of Technology Minna
108 PUBLICATIONS **1,466** CITATIONS
SEE PROFILE

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

BRIEFINGS FROM THE RESEARCH ADVISORY GROUP

BRIEFINGS TO THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE FOR THE FULL COMMISSION MEETING, NEW DELHI 2017

New Delhi, November 2017

GCSC **ISSUE BRIEF №1**

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

PROMOTING STABILITY IN CYBERSPACE TO BUILD PEACE AND PROSPERITY

The Global Commission on the Stability of Cyberspace (GCSC) engages the full range of stakeholders to develop proposals for norms and policies to enhance the international security and stability of cyberspace.

@theGCSC

www.cyberstability.org

info@cyberstability.org

cyber@hcss.nl

The GCSC does not specifically endorse the respective publications, nor does it necessarily ascribe to the findings or conclusions. All comments on the content of the publications should be directed to the respective authors.

This work was carried out with the aid of a grant from GCSC partners: the Ministry of Foreign Affairs of the Netherlands, Cyber Security Agency of Singapore, Microsoft, ISOC, Ministry of Foreign Affairs of France. The views expressed herein do not necessarily represent those of the partners.

The Hague Centre for Strategic Studies

Lange Voorhout 1
2514 EA The Hague
The Netherlands

info@hcss.nl
HCSS.NL

EastWest Institute (EWI)

www.eastwest.ngo
communications@eastwest.ngo

ABOUT THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

The Global Commission on the Stability of Cyberspace (GCSC) helps to develop norms and policies that advance the international security and stability of cyberspace. It promotes mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity. By finding ways to link the various intergovernmental dialogues on international security with the new communities created by cyberspace, the GCSC fulfils a critical need: supporting policy and norms coherence related to the security and stability in and of cyberspace by applying a multi-stakeholder approach to its deliberations on peace and security.

Chaired by Marina Kaljurand, and Co-Chairs Michael Chertoff and Latha Reddy, the Commission comprises 26 prominent Commissioners representing a wide range of geographic regions as well as government, industry, technical and civil society stakeholders with legitimacy to speak on different aspects of cyberspace.

The GCSC Secretariat is provided by The Hague Centre for Strategic Studies and supported by the EastWest Institute.

ABOUT THE BRIEFINGS

The briefings and memos included in this issue were developed by independent researchers working within the GCSC Research Advisory Group. The papers included here were submitted to the Global Commission on the Stability of Cyberspace (GCSC) in order to support its deliberations.

The opinions expressed in the publications are those solely of the authors and do not necessarily reflect the views of the GCSC, its partners, or The Hague Centre for Strategic Studies. The Commission does not specifically endorse the respective publications, nor does it necessarily ascribe to the findings or conclusions. All comments on the content of the publications should be directed to the respective authors.

The research was commissioned by the GCSC in a Request for Proposal after its Commission Meeting in Tallinn in June 2017. The Commissioners selected the winning proposals at the Commission Meeting in Las Vegas in July 2017. The researchers received the funding associated with the Request for Proposal and were invited to present their work to the Commissioners during the Commission Meeting in New Delhi in November 2017.

TABLE OF CONTENTS

PROTECTING THE CORE

Mr. Oluwafemi Osho, *Federal University of Technology, Minna, Nigeria*

Dr. Joseph A. Ojeniyi, *Federal University of Technology, Minna, Nigeria*

Dr. Shafi'l M. Abdulhamid, *Federal University of Technology, Minna, Nigeria*

BRIEFING №3

TABLE OF CONTENTS

SUMMARY

The Internet is a global network consisting of autonomous and interconnected computer networks. At its core are backbone protocols and infrastructures. Over the years, the Internet has become target of inappropriate behaviors by both state and non-state actors. It has been increasingly subjected to significant threats and disruption. This briefing presents a summary of the most significant risks to the stability and security of the Internet, and the existing mechanisms to mitigate them. The methodology combines the use of extensive literature survey and perception of relevant communities that manage the core infrastructure of the Internet. It suggests that the loss or degradation of the core systems that provide basic Internet services is bound to have severe consequences on the functionality of the Internet. Consequently, it becomes pertinent that the core Internet infrastructures should be safeguarded against threats and interventions that exploit, undermine or target them.

SECTION 1: INTRODUCTION

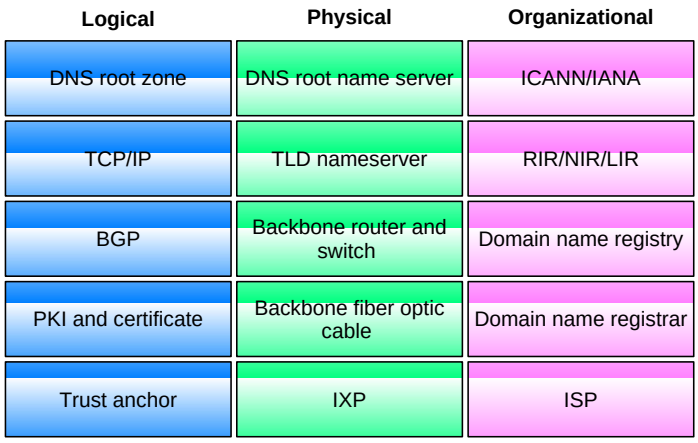
The Internet is a global network consisting of autonomous and interconnected computer networks. Over the years, significant evolution has been recorded in the technological, operations and management, social, and commercialization aspects of the Internet (Leiner et al. 2009). Essentially, it provides communication and information services (Maier and Wildberger 1994), supporting device to device, user to user, and user to device communication, and serving as a repository of information. Regular services provided by the Internet, under the two main categories, include, but not limited to, electronic mails, telnet, mailing list, chat, newsgroup, World Wide Web (WWW), file transfer protocol (FTP), and Gopher/WAIS/Archie/Veronica.

The success of the Internet, to a large extent, has been due to the trust its users have placed on its availability, consistency, and integrity. At the root of this trust are core values of accessibility, universality, operational stability, reliability, security, resiliency, and global interoperability expected by users (ICANN 2014b; Broeders 2015a; Internet Society 2017a).

1.1 THE CORE OF THE INTERNET

At the core of the Internet are protocols and infrastructures. These are consisted in systems that make up the logical, physical, and organizational infrastructure, which provide core naming and forwarding functions (Broeders 2017), ensuring the functionality and integrity of the Internet. These key protocols and infrastructures include (as shown in Figure 1), among other things, DNS root zone; DNS root server; TLD name servers; communication protocols: TCP/IP; routing protocols (e.g. BGP); PKI and certificates; routing facilities: core routers and switches, backbone fiber cables, Communication satellite; service providers: ISPs, IXPs; Internet administration/maintenance: ICANN/IANA; Internet registration: RIRs, domain name registry and registrars; and Internet standards developer: IETF (Hall 2000; Lévy-Bencheton et al. 2015; Bush et al. 2010; US GAO 2006; Internet Society 2017b; Biddle 2012).

Figure 1. Some Internet core protocols and infrastructure



However, over the years, the Internet has become target of inappropriate behaviors by both state and non-state actors. Its stability and security are continually subjected to significant threats and disruptions. In the past, Internet governance used to be the business of the technical community. Today, however, states are getting much more involved. Governance of the Internet has become more of governance using the Internet (Broeders 2015a).

1.2 RESEARCH OBJECTIVES

This research aims to present a summary of the most significant risks of global Internet disruption to the stability and security of the Internet and the corresponding mitigation measures. To achieve this aim, the specific objectives are to:

i. Present a formal definition and taxonomy of disruption of Internet services.

ii. Present significant risks to the core of the Internet.

iii. Present existing techniques and recommended good practices for mitigating the risks.

iv. Propose recommendations to enhance stability and security of the Internet.

1.3 RESEARCH STRUCTURE

The rest of the brief is organized as follows: chapter two focuses on defining and categorizing disruption to regular Internet services. The most significant risks to the core of the Internet are presented in chapter three. Chapter four discusses the risk mitigation mechanisms. Some recommendations towards enhancing stability and security of the Internet are presented in chapter five. The research concludes highlighting the implications of the foregoing on the definition of the public core of the Internet.

1.4 RESEARCH METHODOLOGY

This brief combines the use of extensive literature survey and perception of relevant community that manages the core infrastructure of the Internet. The research items were collated from relevant reports and literatures. The views of the expert were captured via email survey. Specifically, different questions sought their opinions on definition of disruption of Internet services; different threats, their respective level of impact and likelihood of occurrence; and level of effectiveness of existing risk mitigation techniques and recommended good practices. However, due to high variability in the perception of the experts on the aspects of threats and mitigation, only their views on Internet service disruption definition were considered.

SECTION 2: DISRUPTION OF INTERNET SERVICES

This chapter defines the concept of Internet disruption and identifies different forms of disruption – both conventional and non-conventional. To formulate a definition for Internet services disruption, survey respondents were asked, via an open-ended question, to define the term "significant disruption of regular Internet services" on a national or regional scale. From the responses, most frequently occurring terms were identified. These formed the basis of the proposed definition.

2.1 DEFINITION OF DISRUPTION OF REGULAR INTERNET SERVICES

Disruption of the Internet, at the very least, impinges on its capacity to provide needed services. However, its scope (in terms of users affected), scale (magnitude of effect), and period (amount of time) must be significant.

From the foregoing, the following definition of Internet disruption is proposed:

> A security breach that affects significant number of users, over a significant amount of time, causing significant impediment, interruption or retardation of access to, free flow of information through, or services provided by, the Internet.

2.2 TAXONOMY OF INTERNET DISRUPTION

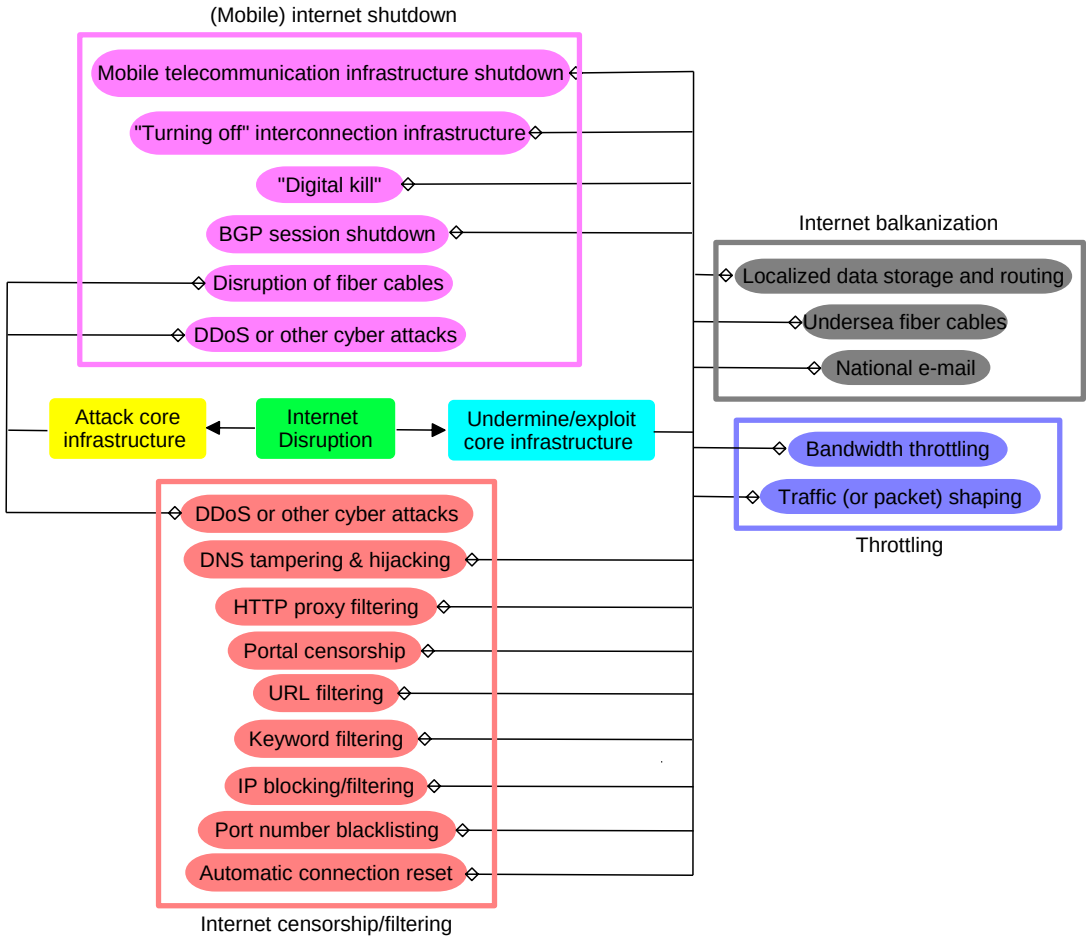
The Internet was designed as a decentralized system, with its contents unregulated, and access to it unmonitored (Amichai-Hamburger 2013). By nature it is meant to be open, distributed and interconnected (Maurer et al. 2014). These properties are essential for the Internet to continuously guarantee the confidentiality, integrity, and availability of users' information, and consequently maintain its indispensability in the foreseeable future. Therefore, any behavior or activity that negatively impacts these characteristics can be categorized as disruptive to the Internet.

One potential impact of Internet disruption is countermining the functionality and integrity of the Internet (Broeders 2015a). Some of the consequences are reduced users' confidence in the Internet and Internet usage. Reports have shown that existing users already are increasingly becoming concerned about their privacy and security (Kende 2016).

Broadly speaking, regular Internet services can be disrupted by either undermining/exploiting or attacking core Internet protocols and infrastructures. As a result of these, different forms of disruption can be identified, viz. national or sub-national (mobile) Internet shutdown (West 2016), national or sub-national Internet censorship/filtering, throttling (Deloitte 2016; Aydin 2016), and Internet balkanization (Kumar 2001; Van Alstyne and Brynjolfsson 1996; Flew 2017; Maurer et al. 2014; Chander and Le 2014; Chander and Le 2015). Each of these disruptions requires different techniques, activities or behaviors to undermine, exploit or attack core Internet protocols and/or infrastructures. Figure 2 presents identified types of Internet service disruption, with the corresponding mechanisms used.

Table 1 highlights the different types of Internet service disruption, technique employed, what is disrupted, who disrupts, and the incentives and disincentives for disrupting these services

Figure 2. A taxonomy of Internet services disruption



(MOBILE) INTERNET SHUTDOWN

This involves the temporary shutting down of the entire Internet or mobile Internet, and may cover the entire or certain regions of a country. A typical example is the shutting down by the Egyptian government, in 2011, of the entire Internet for a period of 5 days, to stifle protest (West 2016).

Techniques used by state actors include shutting down telecommunication infrastructures or BGP session, powering down core devices, or changing the routing tables ("digital kill") (Wolchover 2011; Decraene et al. 2011; Van Beijnum 2011). These would normally target core devices like routers, switches, and telecommunication infrastructures. Non-state actors, on their own part, target fiber cables, and employ DDoS and other cyber attacks against the core devices (Sigholm 2013).

Apart from separating Internet users from their online acquaintances, Internet shutdowns negatively impact economic activities (West 2016). The economic impact has been estimated at an average of $23.6 million per 10 million population for a highly Internet-connected country (Deloitte 2016).

INTERNET CENSORSHIP/FILTERING

Internet censorship simply implies the control or stifling of contents on the Internet. This behavior is commonly employed by authoritarian governments, who enlist the service of service providers, to control the information accessible on the Internet (Leberknight et al. 2010; Broeders 2015b). The censorship could be applied nationally or limited to specific regions. Core Internet assets targeted includes gateway, domain name and web servers, and core routers.

To censor the Internet, techniques commonly employed are DNS tampering, HTTP proxy filtering, IP blocking/filtering, keyword filtering, URL filtering (Terman 2012; Faris and Villeneuve 2008; Leberknight et al. 2010; Dutton et al. 2011); DDoS, web defacement, and other cyberattacks against websites and contents (Noman 2011; Colarik and Ball 2016; Schmidt and Cohen 2014). A case study of the use of DDoS to enforce censorship is the use of 'the Great Canon' by government of China (Essers 2015).

THROTTLING

Throttling can be described as disruptions implemented through reductions in speed of the entire or specific services of the Internet. This significantly elongates the average time it takes a user to access a resource on the Internet. In some cases, certain services on the Internet may be rendered unusable once the speed is reduced below a particular level (Deloitte 2016).

Regrettably, this form of disruption is increasingly gaining preference, due to its less detectability, among state actors who try to limit free flow of information (Kelley 2017). In 2017, to curtail the spread of rumours, the Indian government requested Telecom companies to downgrade 3G and 4G services to 2G speeds (Shashidhar 2017).

Slowing down of the Internet can be implemented on core routers and servers, and other broadband infrastructure by regulating the rate of flow of packet to a certain quality level. This technique is known as traffic (or packet) shaping. It exists in the form of bandwidth throttling and rate limiting, depending on whether the regulation affect data transfer in or out of the network (TechTarget Network 2010).

INTERNET FRAGMENTATION

Internet fragmentation, also referred to as Internet balkanization (Maurer and Morgus 2014; Ma et al. 2010) or splintering the Internet (The Economist 2010), is the creation of "parallel Internets that would be run as distinct, private, and autonomous universes." (Kumar 2001). Three forms of fragmentation have been proposed: technical, governmental, and commercial fragmentation (Drake, Cerf, and Kleinwachter 2016). This brief focuses on the governmental fragmentation, which essentially centers on Internet border controls established to keep data in (Chander and Le 2014). To actualize this, different recommendations have been tabled, viz. creation of national email, localization of data storage and routing, and construction of new undersea cables (Maurer et al. 2014).

Fragmenting the Internet, for instance towards Internet/data nationalism, could require interfering with routing protocols (Broeders 2015b). This distorts the Internet's architecture. Localized e-mail and data storage and routing, among other things, impose geographical boundaries on traffic. This undermines the open and interconnected structure of the Internet (Maurer et al. 2014).

INCENTIVES/DISINCENTIVES FOR DISRUPTING

A close observation of the different case scenarios of disruption of Internet services reveals that authoritarian and repressive state actors disrupt mostly by undermining or exploiting core Internet protocols and infrastructures. On the other, non-state entities, perhaps due to lack of direct access to or control over those core infrastructures, primarily disrupt using attacking against the infrastructures.

Both state and non-state actors have their respective reasons for disrupting the Internet. The incentives and disincentives for state actors to disrupt the Internet fall broadly under three categories: politics and power, social norms and morals, and security concerns. Thus, it is not uncommon to find governments citing national security, prevention of election fraud, false information during elections or examination cheating, maintenance of public order, preservation of social norms and morals, economic interests, or copyright protection in order to shut down, censor or throttle the Internet (Aydin 2016; Broeders 2015a; West 2016; Faris and Villeneuve 2008). For repressive governments, Internet censorship is another veritable instrument for political oppression and suppression (Schmidt and Cohen 2014).

In the case of Internet fragmentation, the incentives are similar. Apart from national security, others are technological sovereignty, protection against foreign surveillance, and of privacy and data (Maurer et al. 2014; Drake, Cerf, and Kleinwachter 2016).

On the other hand, for non-state actors, their motives differ. Attacking Internet infrastructure, websites, or contents are motivated by economic/financial gain, revenge, grievance, sabotage, need for political or social change, propagation of propaganda, or patriotism (Sigholm 2013).

2.3 OTHER INTERNET "MISUSE" THAT DISRUPT

There are other activities that constitute a covert disruption of Internet services. They comprise of Internet abuse or misuse. In essence, these equally erode users' trust and affect how they use the Internet.

One of these is Internet surveillance. It requires exploiting core Internet protocols (Broeders 2015b) and infrastructure. Techniques used include bulk collection, illegal wiretapping, and packet sniffing. While it does not directly impinge on accessibility, it countermines confidentiality and integrity of data. When Internet users become aware that their conversations are under surveillance by the government, their willingness to express themselves freely and socially interact online might be stifled.

Table 1. Disruption techniques and actors, disrupted assets, and motivations for disrupting Internet services

Type	Technique	Asset targeted	Actor	Incentive/ Disincentive
National or sub-national (mobile) Internet shutdown	Shutting down mobile telecommunication infrastructure	telecommunication infrastructure	Governments, ISPs	National security, election fraud, false information during elections, public order, examination cheating prevention
	"Turning off," e.g. powering down or unplugging interconnection infrastructures or network disconnection	Servers, core routers, network switches		
	"Digital kill," e.g. changing routing tables	Core routers		
	BGP session shutdown	BGP peering links, border router		
	Disruption of fiber cables	Undersea and land cables	Terrorists	Propaganda, protest, revenge, sabotage, political or social change, patriotism, economic/financial gain, grievance
	DDoS or other cyber attacks against the infrastructure of the Internet	Servers, core routers	Hackers, hacktivists, cyber terrorists	

Type	Technique	Asset targeted	Actor	Incentive/ Disincentive
National or sub-national Internet censorship/filtering	IP blocking/filtering	Domain name, web servers, and core routers	▪ Government, ISPs ▪ Hackers, hacktivists, cyber terrorists	▪ National security, social norms and morals, economic interests, copyright protection, political oppression and suppression. ▪ Propaganda, protest, revenge, sabotage, political or social change, patriotism, economic/financial gain, grievance
	DNS tampering/poisoning and hijacking			
	HTTP proxy filtering			
	URL filtering			
	Automatic connection reset			
	Keyword filtering			
	Portal censorship			
	Port number blacklisting			
	DDoS or other cyber attacks against specific sites or contents			
Throttling	Traffic (or packet) shaping: bandwidth throttling and rate limiting	Core routers, servers, broadband infrastructure	Governments, ISPs	National security
Internet fragmentation	National e-mail	Servers, core routers, fiber cables	Governments, ISPs	National security, Technological sovereignty, foreign surveillance prevention, privacy and data protection
	Localization of data storage and routing			
	undersea cables			

SECTION 3: RISKS TO THE STABILITY AND SECURITY OF THE INTERNET

Extending the ICANN's security, stability and resiliency (SSR) framework definition (ICANN 2013) to the entire Internet, stability can be said to be the capacity of the Internet to function as expected. This implies constancy in its character (performance). Security of the Internet, on the other hand, entails protection of the Internet against attacks and misuse. This guarantees confidentiality, integrity, and availability of users' information.

This chapter presents threats to the core Internet infrastructure that negatively impact the stability and security of the Internet. It also identifies systems whose loss or degradation is likely to have severe impact on the Internet.

To identify the threats, relevant published materials were collated. The threats are sectionalized under different categories, viz. deliberate shutdowns; censorship; fragmentation; DNS threats; routing threats; certificate threats; physical attack/disaster; and error, malfunction, and compromise.

3.1 RISK MODEL

According to ISO/IEC 27005 (ISO 2011), information security risk is defined as:

"Potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization."

Table 2 contains different threats to the Internet core, the asset targeted and real-life incidences (Lévy-Bencheton et al. 2015; ICANN 2014a; Piscitello 2016; Turner, Polk, and Barker 2012).

In addition to popular threat, new threats are emerging. An example is the BGP MITM attack. Even though its possibility has been demonstrated since 2009 (Hepner and Zmijewski 2009), it was not until 2013 that these attacks were actually discovered (Alaettinoglu 2015). Another emerging threat is domain shadowing (Team RiskIQ 2016; ICANN 2016). Criminals use stolen or phished registrant's credentials and create large number of unauthorized subdomains, which are used for malicious activities.

3.2 "SINGLE POINT OF FAILURE"

The ISO guide (ISO 2011) described risk as "often characterized by reference to potential events and consequences, or a combination of these." One of the potential events with Internet infrastructure is their loss (which may be due to theft or attack) or degradation. This potentially could constitute a single point of failure.

A single point of failure (SPOF) is a component of a system which, if it fails, causes the entire system to stop functioning (Dooley 2009). To categorize a core Internet infrastructure as, potentially, a single point of failure, if lost or degraded, different perspectives could be considered. One perspective is to assess the criticality of such system to the stable and secure functioning of the Internet. It considers the questions: Can the Internet cope without the system? Are there alternative systems that perform the same functions? If a system is one alternative among systems that perform a

particular function or set of functions, the loss or degradation of that system cannot be expected to cause as much damage to the Internet as when such function or set of functions are performed solely by a single system.

If this yardstick is used, the loss or degradation of any of the infrastructures used to provide or support basic Internet communication and information services could, in theory, constitute a single point of failure. These include the DNS root zone, DNS root name server, TCP/IP, BGP, TLD nameservers, backbone routers, and the companies (as a whole) that manage core infrastructures of the Internet. If the DNS fails, there would be no way to find IP address. Consequently, Internet services become inaccessible (Cooper 2016). In the same vein, "killing" the BGP renders impossible routing of information. And needless to say, destruction of the entire organizations that manage those core infrastructures would inevitably lead to the destruction of the infrastructures too.

The other perspective considers the likelihood of loss or degradation of a system – the effort, cost or time required to cause the loss or degradation – in determining whether a system could be categorized as a single point of failure. Going by this perspective, it will be tempting to conclude that it is near impossible to have any single point of failure. This is due to the existing resiliency level of the Internet. However, considering the increasing acquisition and proliferation of cyberweapons, especially by state actors (Dévai 2016; Hughes and Colarik 2016), the possibility of successfully bringing down a core system, regardless of its level of resiliency, might not be as remote as it is currently believed. Evidences attest to this possibility. Already, some actors (most probably state actors) seem to be mooting the idea of taking down the entire Internet (Paganini 2016; Schneier 2016). Schneier reported about calibrated attacks targeted against organizations that manage core infrastructures of the Internet. The attacks were aimed at determining the limit of their defenses. Another evidence: a group of researchers introduced a DDoS attack, termed Coordinated Cross Plane Session Termination (CXPST), capable of targeting all core routers on the Internet (Schuchard et al. 2010; Mohan 2011).

Table 2. Threat categories, types, assets targeted and real-life scenarios

Threat Category	Threat	Asset Targeted	Case Study
Deliberate shutdowns	Shutting down mobile telecommunication infrastructure	Telecommunication infrastructure	There were more than 50 Internet shutdowns in 2016 alone (Kamen 2017).
	"Turning off," e.g. powering down or unplugging interconnection infrastructures or network disconnection	Servers, core routers, network switches	
	"Digital kill," e.g. changing routing tables	Core routers	
	BGP session shutdown	BGP peering links, border router	
Censorship	IP blocking/filtering	Domain name and web servers, core routers	Iran is ranked 1st in terms of Internet censorship. In China, using a 4-level filtering process, government block more than 1 to 4 sites accessible via search engines (Gaille 2017).
	HTTP proxy filtering		
	URL filtering		
	Automatic connection reset		
	Keyword filtering		
	Portal censorship		
	Port number blacklisting		
	Traffic (or packet) shaping: bandwidth throttling and rate limiting	Core routers, servers, broadband infrastructure	Iran in 2009 (Anderson 2013) and 2013 (Aryan, Aryan, and Halderman 2013).
Fragmentation	National e-mail	Servers, core routers, fiber cables	Iran launched its own Youtube; Turkey intends to build a domestic search engine and email service (Clark et al. 2017).
	Localization of data storage and routing		

Threat Category	Threat	Asset Targeted	Case Study
DNS threats	Brute-force attack	Root zone KSK	
	Substitution attack	Root zone KSK	
	Pre-image attack	Root zone KSK	
	Domain shadowing attack	Domain registrant credentials	Use of Angler Exploit Kit (Biasini 2015).
	DNS cache poisoning attack	DNS resolvers	Google Malaysian domain hit with DNS cache poisoning attack (Previous Contributors 2013)
	DNS hijacking attack	DNS server	Wikileaks site hacked via its DNS (Greenberg 2017).
	"Exploit to own" DoS attack	Name servers	Attacker could execute arbitrary code (Manion 2003).
	DDoS attack	Core servers	All 13 DNS root servers targeted (Roberts 2002)
	DNS amplification attack	Servers, end-user nodes	An attacker sends at least 20Gbps against an end-user's system 24 hours a day (Prince 2012).
	Malware	Core servers	Malware-based DDoS attack against Dyn servers (Woolf 2016)
	Domain registration hijacking attack	Registration account, Name servers	PANIX became a victim of domain hijacking (SSAC 2005).
	DNS response modification	DNS resolver	

Threat Category	Threat	Asset Targeted	Case Study
Routing Threats	BGP route leak	Autonomous systems	Misconfigured router caused Internet service degradation (Madory 2017)
	BGP (prefix) hijacking attack	Autonomous systems	Tens of prefixes originated from Rostelecom (Toonk 2017)
	BGP MITM attack	Autonomous systems	Traffic for major networks directed to an ISP in France (Toonk 2013)
Certificate threats	Impersonation	Certificates	
	Registration Authority compromise	Certificates	
	Certificate Authority system compromise	Certificates, Certificate revocation lists (CRLs)	DigiNotar CA breach (Hoogstraaten et al. 2012).
	CA Signing key compromise	CA signing key, certificates, CRLs	
Physical attack/disaster	Vandalism/theft/loss	Undersea and land cables and other core infrastructure	Fiber cables in California attacked (T. Hughes 2015)
	Natural/Environmental disaster	Core physical infrastructure	Under-sea cable damaged by powerful earthquakes off the coast of Taiwan (Lemon 2006).
Error, malfunction, compromise	Root/TLD operator errors	Root/TLD infrastructure	
	Hardware failure	Core physical infrastructure	
	Registration services failure/compromise	Services	
	Service provider failure/operation disruption	Hardware, software, services	

SECTION 4: MITIGATING RISKS TO THE STABILITY AND SECURITY OF THE INTERNET

This chapter focuses on highlighting some of the existing techniques and recommended best practices for mitigating risks to the core of the Internet.

A number of the threats to the Internet, often employed by authoritarian or repressive state actors, are not direct attacks. Core Internet infrastructure are exploited or undermined. These equally destabilize and undermine the security of the Internet. For these threats, there are no formal recommended good practices. However, Internet users have devised different informal methods of dealing with them. One of these threats is censorship. Tools commonly used to bypass censorship include Virtual Private Networks (VPNs), custom DNS servers, web-based proxies, Tor browser, and SSH tunnels (Hoffman 2016). In 2014, an Android-based app, DNSet, was used by Turkish citizens to bypass censorship during the first months. The application enabled users who did not have administrative rights on their devices to alter, without difficulty, the DNS server imposed by 3G/4G providers (Di Florio et al. 2014).

For threats like deliberate shutdown and Internet fragmentation, there are no technical countermeasures to mitigate them. new methods might be required to moderate them.

Some of the existing recommendations for mitigating threats that target core infrastructure are presented in Table 3 (Internet Society, n.d.; Lévy-Bencheton et al. 2015; Conrad 2016; IANA 2016; US-CERT 2013; Xu 2017; Manion 2003; SSAC 2005; SSAC 2008; Turner, Polk, and Barker 2012; Lewis 2017; Qamar 2014; Khanse 2015).

4.1 GAPS

Despite the array of techniques and mechanisms available to prevent and mitigate many of the threats to the core infrastructure of the Internet, there are issues that require attention. One of these is root zone KSK rollover. It was meant to take place on October 11, 2017, but had to be postponed. Some implementation and configuration bugs associated with RFC 5011, the mechanism which enables validators to automatically update their trust anchors, were discovered (Wessels 2017).

Another issue is the limitation of the DNSSEC. It essentially addresses the aspect of integrity. Other aspects of information security, including confidentiality of the information inside the DNS and availability needs to be addressed. Much efforts are still required to ensure the network layer of the infrastructure are protected (Marsan 2010).

Equally worthy of further attention are the emerging threats. While a number of mitigation mechanisms have already been proposed (Huston 2013; Oti, Bansah, and Adegboyega 2016), more research is needed to address issues that might arise during their implementation.

Table 3. Risk mitigation techniques and good practices

Threats	Mitigation Technique/Good Practices
DNS Threats	
Brute-force attack	Periodic changing of the root zone-signing cryptographic keys.
Substitution attack	Distribute the public component of a Trust Anchor in a secure fashion.
Pre-image attack	Implement a sufficiently resistant cryptographic hash function in conjunction with the signing algorithm during the time in which the signature is valid.
Domain shadowing attack	Check IP addresses against a reputation-based blacklist if it resolves to multiple names or IP addresses.
	Adopt heuristic behavioral analysis to identify potentially malicious network connections requiring further inverstigation.
DNS cache poisoning attack	Adopt DNS open resolver configuration.
	Deploy DNSSEC for securing DNS clients origin authentication of DNS data, authenticated denial of existence and data integrity.
	Utilize developed patches commonly adopted against Kaminsky Cache Poisoning.
	Restrict zone transfers to reduce load on systems and network.
DNS hijacking attack	Apply DNSSEC.
	Use good security software capable of preventing DNS-Changing malware.
"Exploit to own" DoS attack	Upgrade or apply vendor-specified patch.
	Restart dynamically linked processes and recompile statistically linked libraries.

Threats	Mitigation Technique/Good Practices
DDoS attack	Apply BCP38 to mitigate DDoS attacks via IP Source Address Spoofing.
	Adopt source IP address verification at the edge of Internet infrastructure.
	Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure
	Disable open recursion on name servers and only accept DNS queries from trusted sources.
	Manufacturers and configurators of network equipment should take steps to secure all devices, e.g. keep them up-to-date by patching flaws.
DNS amplification attack	ISP should reject any DNS traffic with spoofed addresses.
	Disable recursion on authoritative name servers.
	Restrict recursion to only authorized clients.
Malware	Use strong anti-malware software and also update your system and software periodically.
Domain registration hijacking attack	Registries should implement Registrar-Lock and EPP authInfo according to specification.
	Resellers and registrants should be provided with Best Common Practices by registries and registrars that describe appropriate use and assignment of EPP authInfo codes and risks of misuse.
	An emergency action channel should be provided by registrars.
DNS response modification	Inquiry should be made by registrants about the treatment of their unregistered subdomains by entrusted agents.
	Organization for which accurate NXDomain reporting is essential for operational stability should opt for entrusted agents that guarantee non-modification of DNS responses in its terms of service.
Routing Threats	
BGP route leak	Announce routes more preferable than leaked route to counter illegitimate routes.

Threats	Mitigation Technique/Good Practices
BGP route leak	Entirely change prefix via modifying DNS records.
	Route Origin Authorizations (ROAs) should be published in the various RIRs.
BGP (prefix) hijacking attack	Apply cryptographic resource certification (RPKI) for the purpose of AS origin validation.
	Establish an Appropriate Use Policy (AUP) to promote rules to secure peering.
	Utilize resource information from databases such as IRR, APNIC, ARIN, and RIPE.
	Utilize prefix filtering and automation of prefix filters.
	Utilize prefix filters to facilitate validation of routing information on global scale.
	Utilize third-party BGP prefix hijacking detection service from which you receive notifications (please, note that this mitigation is under debate).
BGP MITM attack	Periodic changing of the cryptographic keys used to sign the root zone.
Certificate Threats	
Impersonation	RAs must ensure adoption of best practices for vetting certificate requests as documented in the certificate policies (CPs) associated with the CAs served by the RA.
RA compromise	RAs must implement security best practices.
CA system compromise	CAs must perform regular third-party audits and reviews.
	CAs must implement mechanisms for tracking and detection and perform regular manual operational sanity checks.
	CAs must revoke issued fraudulent certificates, when detected, and inform victim organizations and all potential relying parties.
CA signing key compromise	In the event of a signing key theft, CAs must revoke all certificates issued by the compromised CA and all necessary parties notified that they would require new certificates.

SECTION 5: ENHANCING THE STABILITY AND SECURITY OF THE INTERNET

Previous chapters have discussed essentially various risks to the stability and security of the Internet and some of the existing strategies to mitigate them. The capacity of the Internet to sustain its underlying values of universality, interoperability, and accessibility is firmly hinged on continuous guarantee of the functionality and integrity of its core components (Broeders 2015a; Broeders 2015b).

This chapter proposes some measures essential towards improving the stability and security of the Internet.

- More efforts are required in the area of detection or/and mitigation of threats including BGP MITM, root zone KSK brute-force, and domain shadowing attacks. Existing solutions need further reviews. For instance, while it is certain the root zone KSK rollover is essential to mitigate brute-force attack against the KSK, further research could be commissioned towards identifying potential implementation and configuration issues.
- The size and scale of recent cyberattacks are pointing to increasing involvement of state actors. When this is placed side by side the increasing critical role the Internet is likely to play in national development in the years ahead, the need for states to categorize security of the Internet as a national security issue, more than ever before, cannot be overemphasized. Hence, states should identify all core Internet infrastructures within their boundaries as critical national infrastructure (CNI). While some states, including UK (CPNI 2017) and US (DHS 2017), have included communication sector or/and IT sector as CNIs, others, like Nigeria (Adepetun 2016; Onwuanumba 2017), are yet to.

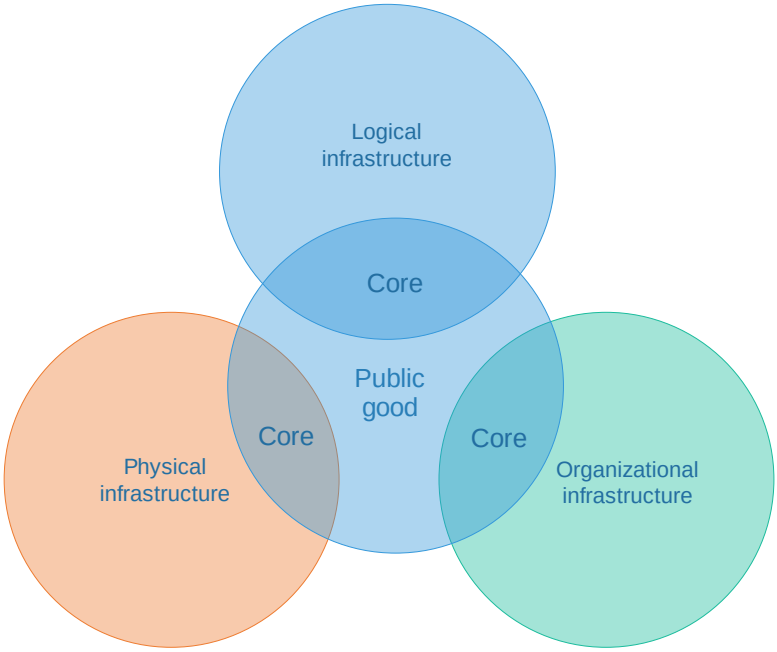
CONCLUSION: IMPLICATIONS FOR THE "PUBLIC CORE" OF THE INTERNET

This brief identifies the various categories of Internet disruption and risks which threaten the core infrastructure of the Internet. Existing risk mitigation mechanisms and good practices are explored; while some gaps, requiring urgent attention, are identified. Lastly, some measures essential to enhance the stability and security of the Internet are proposed.

Using criticality to the stability and security of the Internet as a basis, this brief argues that the systems that support basic information and communication services on the Internet could, if lost or degrade, in theory, constitute single points of failure. These include the DNS root zone, DNS root name server, TCP/IP, BGP, TLD nameservers, backbone routers, and the companies that manage core infrastructures.

The future of the Internet rests primarily on its capacity to consistently guarantee the values of confidentiality, integrity, and availability. The arguments of this brief underline the urgent need for the core infrastructures of the Internet to be protected from belligerent state and non-state actors who undermine, exploit, and target them. This supports existing studies (e.g. Broeders 2015a), which recommend the designation of core Internet protocols and infrastructures as a global public good (as presented in Figure 3). The Internet affords many benefits to everyone. Hence, the core of its existence and survival should not be jeopardized.

Figure 3. The Internet core as a global public good



BIBLIOGRAPHY

Adepetun, Adeyemi. 2016. "For Telecoms Operators, the Challenge of Infrastructure Vandalism Is Sour Pill." The Guardian, April 12. https://guardian.ng/features/for-telecoms-operators-the-challenge-of-infrastructure-vandalism-is-sour-pill/.

Alaettinoglu, Cengiz. 2015. "BGP Security: No Quick Fix." Network Computing. https://www.networkcomputing.com/networking/bgp-security-no-quick-fix/1303232068.

Amichai-Hamburger, Yair, ed. 2013. The Social Net: Understanding Our Online Behavior. Oxford: Oxford University Press.

Anderson, Collin. 2013. "Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran." arXiv Preprint arXiv:1306.4361, 1–31. http://arxiv.org/abs/1306.4361.

Aryan, Simurgh, Homa Aryan, and J. Alex Halderman. 2013. "Internet Censorship in Iran : A First Look." 3rd USENIX Workshop on Free and Open Communications on the Internet, no. August: 8.

Aydin, Deniz Duru. 2016. "Five Excuses Governments (Ab)use to Justify Internet Shutdowns." DW Akademie. http://www.dw.com/en/five-excuses-governments-abuse-to-justify-internet-shutdowns/a-36135649.

Biasini, Nick. 2015. "Threat Spotlight: Angler Lurking in the Domain Shadows." Cisco Blogs. https://blogs.cisco.com/security/talos/angler-domain-shadowing.

Biddle, Sam. 2012. "How to Destroy the Internet." Gizmodo. http://gizmodo.com/5912383/how-to-destroy-the-internet.

Broeders, Dennis. 2015a. The Public Core of the Internet: An International Agenda for Internet Governance. WRR-Policy Brief. The Hague: WRR.

———. 2015b. The Public Core of the Internet: An International Agenda for Internet Governance. Amsterdam: Amsterdam University Press.

———. 2017. "Defining the Protection of 'the Public Core of the Internet' as a National Interest." New Delhi. http://cf.orfonline.org/wp-content/uploads/2017/07/ORF_IssueBrief_190_PublicCore.pdf.

Bush, R, D Karrenberg, M Kosters, and R Plzak. 2010. "Root Name Server Operational Requirements." https://tools.ietf.org/pdf/rfc2870.pdf.

Chander, Anupam, and Uyen P Le. 2014. "Breaking the Web: Data Localization vs. the Global Internet." Emory Law Journal, Forthcoming; UC Davis Legal Studies Research Paper No. 378., no. April: 1–50. doi:http://dx.doi.org/10.2139/ssrn.2407858.

———. 2015. "Data Nationalism." Emory Law Journal 64 (3): 677–739. law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.

Clark, By Justin, Rob Faris, Ryan Morrison-westphal, Helmi Noman, Casey Tilton, and Jonathan Zittrain. 2017. "The Shifting Landscape of Global Internet Censorship." Cambridge, Massachusetts. https://thenetmonitor.org/research/2017-global-internet-censorship#results.

Colarik, Andrew, and Rhys Ball. 2016. "Anonymous Versus ISIS: The Role of Non-State Actors in Self-Defense." Global Security and Intelligence Studies 2 (1): 4. doi:10.18278/gsis.2.1.3.

Conrad, David. 2016. "DNSSEC: Rolling the Root Zone Key Signing Key." ICANN Blog. https://www.icann.org/news/blog/dnssec-rolling-the-root-zone-key-signing-key.

Cooper, David. 2016. "Why Is DNS Important?" Quora. https://www.quora.com/Why-is-DNS-important.

CPNI. 2017. "Critical National Infrastructure." Accessed December 1. https://www.cpni.gov.uk/critical-national-infrastructure-0.

Decraene, P, P Francois, C Pelsser, Z Ahmad, A. J Elizondo Armengol, and T Takeda. 2011. "Requirements for the Graceful Shutdown of BGP Sessions." https://tools.ietf.org/html/rfc6198.

Deloitte. 2016. "The Economic Impact of Disruptions to Internet Connectivity A Report for Facebook." http://globalnetworkinitiative.org/sites/default/files/The-Economic-Impact-of-Disruptions-to-Internet-Connectivity-Deloitte.pdf.

Dévai, Dóra. 2016. "Proliferation of Offensive Cyber Weapons. Strategic Implications and Non-Proliferation Assumptions." AARMS 15 (1): 61–73.

DHS. 2017. "Critical Infrastructure Sectors." Accessed December 1. https://www.dhs.gov/critical-infrastructure-sectors#.

Di Florio, Andrea, Nino Vincenzo Verde, Antonio Villani, Domenico Vitali, and Luigi Vincenzo Mancini. 2014. "Bypassing Censorship: A Proven Tool against the Recent Internet Censorship in Turkey." In 2014 IEEE International Symposium on Software Reliability Engineering Workshops, ISSREW 2014, 389–94. doi:10.1109/ISSREW.2014.93.

Dooley, Kevin. 2009. Designing Large-Scale LANs. O'Reilly Media.

Drake, William J., Vinton G. Cerf, and Wolfgang Kleinwachter. 2016. "Internet Fragmentation: An Overview." Future of the Internet Initiative White Paper. http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

Dutton, William H, Anna Dopatka, Michael Hills, Ginette Law, and Victoria Nash. 2011. "Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet." Paris.

Essers, Loek. 2015. "The 'Great Cannon' of China Enforces Internet Censorship." Computerworld. https://www.computerworld.com/article/2908504/the-great-cannon-of-china-enforces-internet-censorship.html.

Faris, Robert, and Nart Villeneuve. 2008. "Measuring Global Internet Filtering." Access Denied: The Practice and Policy of Global Internet Filtering 5: 1–24. https://opennet.net/sites/opennet.net/files/Deibert_02_Ch01_005-028.pdf.

Flew, Terry. 2017. "When Governments Want to Splinter the Internet." Khaleej Times, August 4. http://www.khaleejtimes.com/opinion-editorial/when-governments-want-to-splinter-the-internet.

Gaille, Brandon. 2017. "33 Amazing Internet Censorship Statistics." Brandon Gaille. https://brandongaille.com/32-amazing-internet-censorship-statistics/.

Greenberg, Andy. 2017. "Hacker Lexicon: What Is DNS Hijacking?" Wired. https://www.wired.com/story/what-is-dns-hijacking/.

Hall, Eric A. 2000. Internet Core Protocols: The Definitive Guide. Edited by Mike Loukides. First. California: O'Reilly & Associates.

Hepner, Clint, and Earl Zmijewski. 2009. "Defending Against BGP Man-In-The-Middle Attacks." In Talk at BlackHat. Arlington, Virginia. https://www.blackhat.com/presentations/bh-dc-09/Zmijewski/BlackHat-DC-09-Zmijewski-Defend-BGP-MITM.pdf.

Hoffman, Chris. 2016. "5 Ways to Bypass Internet Censorship and Filtering." How-To Geeks. https://www.howtogeek.com/167418/5-ways-to-bypass-internet-censorship-and-filtering/.

Hoogstraaten, Hans, Ronald Prins, Daniël Niggebrugge, Danny Heppener, Frank Groenewegen, Janna Wettinck, Kevin Strooy, et al. 2012. "Black Tulip: Report of the Investigation into the DigiNotar Certificate Authority Breach." doi:10.13140/2.1.2456.7364.

Hughes, Daniel, and Andrew M. Colarik. 2016. "Predicting the Proliferation of Cyber Weapons into Small States." Joint Force Quarterly 83: 19–26.

Hughes, Trevor. 2015. "Attacks Show Fiber Optic Internet Cables Vulnerable." USA Today. https://www.usatoday.com/story/news/2015/09/16/attacks-show-fiber-optic-internet-cables-vulnerable/32502785/.

Huston, Geoff. 2013. "MITM and Routing Security." APNIC. https://labs.apnic.net/?p=447.

IANA. 2016. "DNSSEC Practice Statement for the Root Zone KSK Operator." https://www.iana.org/dnssec/icann-dps.txt.

ICANN. 2013. "Security, Stability and Resiliency Framework." https://www.icann.org/en/system/files/files/ssr-plan-fy14-06mar13-en.pdf.

———. 2014a. "ICANN - DNS Resilience Model." https://www.icann.org/en/system/files/files/dns-resilience-model-28may14-en.pdf.

———. 2014b. "ICANN - DNS Risk Assessment." https://www.icann.org/en/system/files/files/dns-risk-consultation-28may14-en.pdf.

———. 2016. "New gTLD Program Safeguards Against DNS Abuse." file:///C:/Users/USER/Downloads/safeguards-against-dns-abuse-18jul16-en (1).pdf.

Internet Society. 2017a. "Internet Resilience and Stability." Accessed December 1. http://internetsociety.ngo/what-we-do/issues/security.

———. n.d. "Mutually Agreed Norms for Routing Security (MANRS)." https://wp.internetsociety.org/routingmanifesto/wp-content/uploads/sites/14/2016/09/MANRS_PDF_Sep2016.pdf.

———. 2017b. "Technical Aspects of the Internet." Accessed September 3. https://www.internetsociety.org/internet/how-it-works/technical-aspects.

ISO. 2011. "ISO/IEC 27005:2011." https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en.

Kamen, Matt. 2017. "Governments Shut down the Internet More than 50 Times in 2016." Wired. http://www.wired.co.uk/article/over-50-internet-shutdowns-2016.

Kelley, Michael B. 2017. "Evidence of Iran â€TM Throttling â€TM the Internet Points to an Ingenious Form of Censorship." Business Insider. http://www.businessinsider.com/how-iran-slows-down-its-internet-2013-6?IR=T.

Kende, Michael. 2016. "Global Internet Report 2016." Internet Society.

Khanse, Anand. 2015. "What Is a DNS Hijacking Attack & How to Prevent It." The WIndowsClub. http://www.thewindowsclub.com/what-is-dns-hijacking-prevention.

Kumar, Aparna. 2001. "Libertarian, or Just Bizarro?" Wired. http://www.wired.com/politics/law/news/2001/04/43216.

Leberknight, Christopher S., Harold Vincent Poor, Mung Chiang, and Felix Wong. 2010. "A Taxonomy of Internet Censorship and Anti-Censorship." In Fifth International Conference on Fun with Algorithms, 28. http://trends.ifla.org/node/25.

Leiner, Barry M, Vinton G Cerf, David D Clark, Robert E Kahn, Leonard Kleinrock, Daniel C Lynch, Jon Postel, Larry G Roberts, and Stephen Wolff. 2009. "A Brief History of the Internet Professor of Computer Science." ACM SIGCOMM Computer Communication Review 39 (5): 22–31.

Lemon, Sumner. 2006. "Earthquakes Disrupt Internet Access in Asia." PCWorld. https://www.pcworld.com/article/128337/article.html.

Lévy-Bencheton, Cedric, Louis Marinos, Rosella Mattioli, Thomas King, Christoph Dietzel, and Jan Stumpf. 2015. "Threat Landscape and Good Practice Guide for Internet Infrastructure." doi:10.2824/34387.

Lewis, Nick. 2017. "What Is Domain Shadowing and How Can Enterprises Defend against It?" SearchSecurity. Accessed December 15. http://searchsecurity.techtarget.com/answer/What-is-domain-shadowing-and-how-can-enterprises-defend-against-it.

Ma, Richard T.B., Dah Ming Chiu, John C.S. Lui, Vishal Misra, and Dan Rubenstein. 2010. "Internet Economics: The Use of Shapley Value for ISP Settlement." IEEE/ACM Transactions on Networking 18 (3): 775–87. doi:10.1109/TNET.2010.2049205.

Madory, Doug. 2017. "Widespread Impact Caused by Level 3 BGP Route Leak." ORACLE + Dyn. https://dyn.com/blog/widespread-impact-caused-by-level-3-bgp-route-leak/.

Maier, G, and A Wildberger. 1994. In 8 Sekunden Um Die Welt. Kommunikation Über Das Internet. Bonn, Paris: Addison-Wesley.

Manion, Art. 2003. "Vulnerability Note VU#844360: Domain Name System (DNS) Stub Resolver Libraries Vulnerable to Buffer Overflows via Network Name or Address Lookups." Vulnerability Notes Database. http://www.kb.cert.org/vuls/id/844360.

Marsan, Carolyn Duffy. 2010. "DNSSEC Doesn't Mitigate All DNS Threats." The IETF Journal, no. October. https://www.ietfjournal.org/dnssec-doesnt-mitigate-all-dns-threats/.

Maurer, Tim, and Robert Morgus. 2014. "Stop Calling Decentralization of the Internet 'Balkanization.'" Future Tense. http://www.slate.com/blogs/future_tense/2014/02/19/stop_calling_decentralization_of_the_internet_balkanization.html.

Maurer, Tim, Robert Morgus, Isabel Skierka, and Mirko Hohmann. 2014. "Technological Sovereignty: Missing the Point?" preview.newamerica.org/downloads/Technological_Sovereignty_Report.pdf.

Mohan, Ram. 2011. "Attacking the Internet's Core." Securityweek Network. http://www.securityweek.com/attacking-internets-core.

Noman, Helmi. 2011. "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army." Information Warfare Monitor. Vol. 30. https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army.

Onwuanumba, Isaiah. 2017. "Nigeria: Govt Sets To Declare Telecoms Facilities 'National Critical Infrastructure.'" IT News Nigeria, March 17. http://www.itnewsnigeria.com.ng/2017/03/17/nigeria-govt-sets-to-declare-telecoms-facilities-national-critical-infrastructure/.

Oti, Stephen Brako, Isaac Bansah, and Tony M. Adegboyega. 2016. "A Configuration Based Approach to Mitigating Man-in- the-Middle Attacks in Enterprise Cloud IaaS Networks Running BGP." International Journal of Computer Applications 146 (1): 23–27. http://www.ijcaonline.org/archives/volume146/number1/oti-2016-ijca-910604.pdf.

Paganini, Pierluigi. 2016. "A Nation-State Actor Is Testing Methods for a Massive Takedown of the Internet According to the Popular Cyber Security Experts an Unknown Nation State Actor May Be Running Tests for Taking down the Entire Internet Infrastructure ." Security Affairs. http://securityaffairs.co/wordpress/51669/hacking/internet-takedown.html.

Piscitello, Dave. 2016. "Attacks Against The DNS." https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/2A.pdf.

Previous Contributors. 2013. "Google's Malaysian Domains Hit with DNS Cache Poisoning Attack." The State of Security. https://www.tripwire.com/state-of-security/latest-security-news/googles-malaysian-domains-hit-dns-cache-poisoning-attack/.

Prince, Matthew. 2012. "Deep Inside a DNS Amplification DDoS Attack." CloudFare. https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/.

Qamar, Ali. 2014. "How to Stop DNS Hijacking." Infosec Institute. http://resources.infosecinstitute.com/stop-dns-hijacking/.

Roberts, Paul F. 2002. "Major 'Net Backbone Attack Could Be First of Many." NetworkWorld. https://www.networkworld.com/article/2342906/lan-wan/major--net-backbone-attack-could-be-first-of-many.html.

Schmidt, Eric E., and Jared Cohen. 2014. "The Future of Internet Freedom." The New York Times. http://www.nytimes.com/2014/03/12/opinion/the-future-of-internet-freedom.html.

Schneier, Bruce. 2016. "Someone Is Learning How to Take Down the Internet." Schneier on Security. http://www.amazon.com/Schneier-Security-Bruce/dp/0470395354.

Schuchard, Max, Abedelaziz Mohaisen, Denis Foo Kune, Nicholas Hopper, Yongdae Kim, and Eugene Y. Vasserman. 2010. "Losing Control of the Internet: Using the Data Plane to Attack the Control Plane." In Proceedings of the 17th ACM Conference on Computer and Communications Security, Pp. 726-728, 1–15. doi:10.1145/1866307.1866411.

Shashidhar, K J. 2017. "Govt Asks Telecom Companies to Throttle Mobile Internet Speeds in Kashmir." Medianama. https://www.medianama.com/2017/06/223-throttle-mobile-internet-speeds-kashmir/.

Sigholm, Johan. 2013. "Non-State Actors in Cyberspace Operations." Journal of Military Studies 4 (1): 1–37. doi:10.1515/jms-2016-0184.

SSAC. 2005. "Domain Name Hijacking: Incidents, Threats, Risks, and Remedial Actions." https://archive.icann.org/en/announcements/hijacking-report-12jul05.pdf.

———. 2008. "SAC 032 Preliminary Report on DNS Response Modification." https://www.icann.org/en/system/files/files/sac-032-en.pdf.

Team RiskIQ. 2016. "Domain Shadowing: When Good Domains Go Bad." RiskIQ. https://www.riskiq.com/blog/external-threat-management/domain-shadowing-good-domains-go-bad/.

TechTarget Network. 2010. "Traffic Shaping (Packet Shaping)." Network Management and Monitoring: The Evolution of Network Control. http://searchnetworking.techtarget.com/definition/traffic-shaping.

Terman, Rochelle. 2012. "Internet Censorship (Part 2): The Technology of Information Control." http://townsendcenter.berkeley.edu/blog/internet-censorship-part-2-technology-information-control.

The Economist. 2010. "The Future of the Internet: A Virtual Counter-Revolution." The Economist. http://www.economist.com/node/16941635.

Toonk, Andree. 2013. "Accidentally Stealing the Internet." BGPMon. https://bgpmon.net/accidentally-stealing-the-internet/.

———. 2017. "BGPstream and the Curious Case of AS12389." BGPMon. https://bgpmon.net/bgpstream-and-the-curious-case-of-as12389/.

Turner, Paul, William Polk, and Elaine Barker. 2012. "Preparing for and Responding to Certification Authority Compromise and Fraudulent Certificate Issuance." http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=911197.

US-CERT. 2013. "DNS Amplification Attacks." US-CERT. https://www.us-cert.gov/ncas/alerts/TA13-088A.

US GAO. 2006. "Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan." Methodology. http://www.gao.gov/assets/260/250483.pdf.

Van Alstyne, Marshall, and Erik Brynjolfsson. 1996. "Electronic Communities: Global Village or Cyberbalkans?" In Proceedings of the 17th International Conference on Information Systems, 1–32. Cleveland, OH. ftp://ftp.gunadarma.ac.id/.upload/www.bogor.net/www.bogor.net/idkf-1/aplikasi/electronic-community-global-village-or-cyberbalkans-03-1997.pdf.

Van Beijnum, Iljitsch. 2011. "How Egypt Did (and Your Government Could) Shut down the Internet." Ars Technica. https://arstechnica.com/tech-policy/2011/01/how-egypt-or-how-your-government-could-shut-down-the-internet/.

Wessels, Duane. 2017. "A Closer Look at Postponing of the Root Zone KSK Rollover Decision." CircleID. http://www.circleid.com/posts/20170929_a_closer_look_at_postponing_of_root_zone_ksk_rollover_decision/.

West, Darrell M. 2016. "Internet Shutdowns Cost Countries $2.4 Billion Last Year." https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf.

Wolchover, Natalie. 2011. "How Do You Shut Down the Internet in a Whole Country?" Live Science. https://www.livescience.com/32965-how-do-you-shut-down-the-internet-whole-country.html.

Woolf, Nicky. 2016. "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say." The Guardian. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

Xu, Young. 2017. "Best Practices to Combat Route Leaks and Hijacks." ThousandEyes. https://blog.thousandeyes.com/best-practices-combat-route-leaks-hijacks/.