



ITHI DNS Sanitas: Sine Morbus

(DNS Health: Free from Diseases) Alain Durand, ITHI, Public Comment Period

ICANN Strategic Plan 2016-2020

https://www.icann.org/en/system/files/files/strategic-plan-2016-2020-10oct14-en.pdf

2.1 Foster and coordinate a healthy, secure, stable, and resilient identifier ecosystem.

KEY SUCCESS FACTORS (OUTCOMES)

- Increased collaboration with the global community that improves the security, stability and resiliency of the unique identifier ecosystem (including updates of the root zone, Internet numbers registries, and protocol parameter registries, operation of the "L" root server, and other operational infrastructure supporting the identifier ecosystem).

- Ecosystem is able to withstand attacks or other events without loss of confidence in the operation of the unique identifier system.
- Unquestionable, globally recognized legitimacy as coordinator of unique identifiers.
- Reduction of government/industry/other stakeholders' concerns regarding availability of IP addresses.



. . .

ITHI Project Timeline

http://www.icann.org/ithi Mailing list: ithi@icann.org

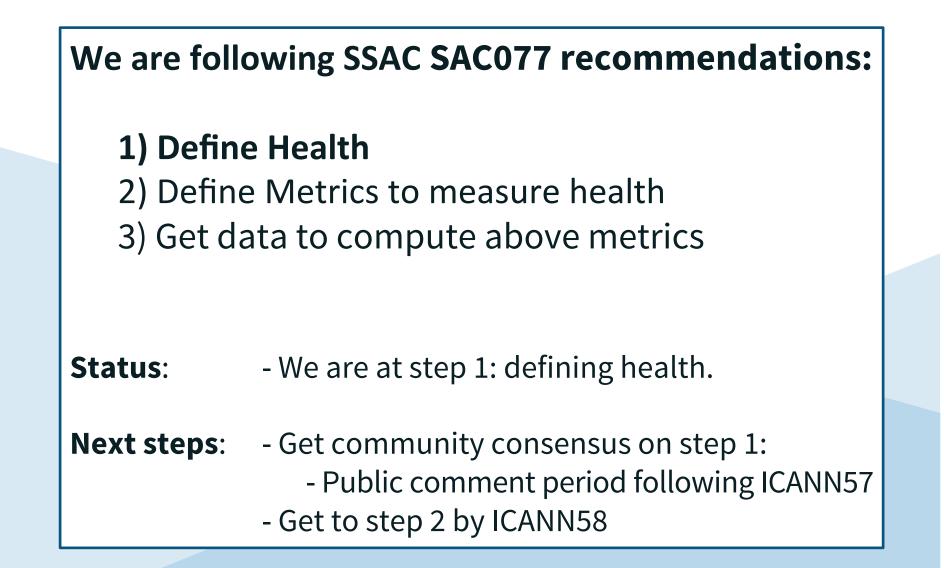
March 2016: ITHI kick-off at ICANN55

Number community, through the NRO, joined the ITHI project but demanded to drive their own component.

September 2016: ITHI workshop at ICANN DC officeOctober 2016: ITHI workshop with M3AAWG, ParisNovember 2016: ITHI session at ICANN57



ITHI: Methodology





Heath: Definition

health |helTH|

noun

the state of being free from illness or injury

- Merriam Webster Dictionary



Describing Diseases: Example from the Mayo Clinic

MAYO CLINIC	Search Mayo Clinic	;		Q	Request an A Find a Docto Find a Job Give Now	or	Log in to Patient Account Translated Content	
PATIENT CARE & HEALTH INFO	DEPARTMENTS & CENTERS	RESEARCH V	EDUCATION	•	FOR MEDICAL PROFESSIONALS	PRODUCTS & SERVICES	GIVING TO MAYO CLINIC	•
	DefinitionCausesSymptomsBy Mayo Clinic StaffCausesThe poliovirus resides only in humans in the feces of someone who's infected primarily through the fecal-oral route, or sanitation is inadequate.Risk factorsComplicationsPreparing for your appointmentPoliovirus can be transmitted through food or through direct contact with sor virus. Polio is so contagious that anyo infected person is likely to become infer				bliovirus spreads cially in areas where aminated water and he infected with the ving with a recently			
	Prevention	← Symptoms		Risk fa	actors \rightarrow		7	6

Definition of Terms

Definition	A statement of the exact meaning of a word
Symptoms	A sign of the existence of something, especially of an undesirable situation
Causes	A person or thing that gives rise to an action, phenomenon, or condition
Risk Factors	A risk factor is any attribute, characteristic or exposure that increases the likelihood of developing a disease or injury.
Complications	A secondary disease or condition aggravating an already existing one
Impact	The effect or influence of one person, thing, or action, on another
Potential Treatment	Treatment: medical care given to a patient for an illness or injury



Latin & Greek Terminology

Sanitas:	Health	
Morbus:	Disease	
sine:	without	
Data:	Data	
Malus:	Bad	
Nefar:	Crime	
Magintudo:	Quantity	
Perfluo:	Leak	
Fallax:	Lying	

-itis: Infection
-Pathy: Disorder
-ism: Condition
-algia: Pain



Heath: Who is the Patient?

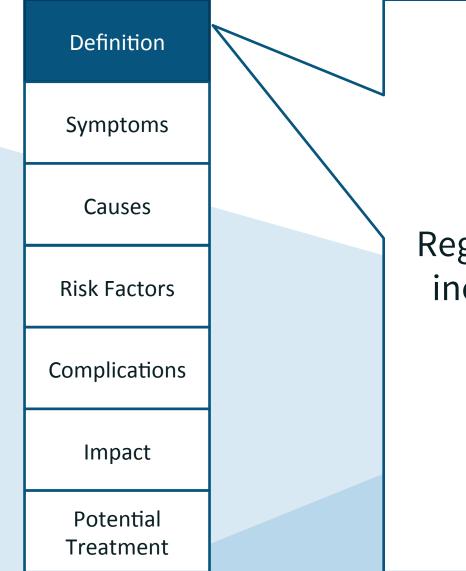
The patient is the system of unique Internet Identifiers ICANN helps coordinate.



Domain Name Abuse Diseases DATAMALGIA (Pain from Bad Data)



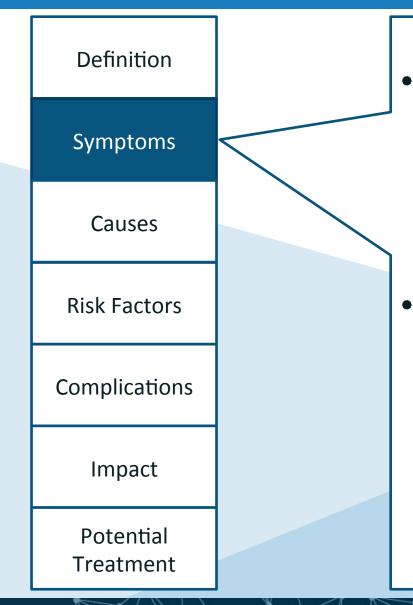




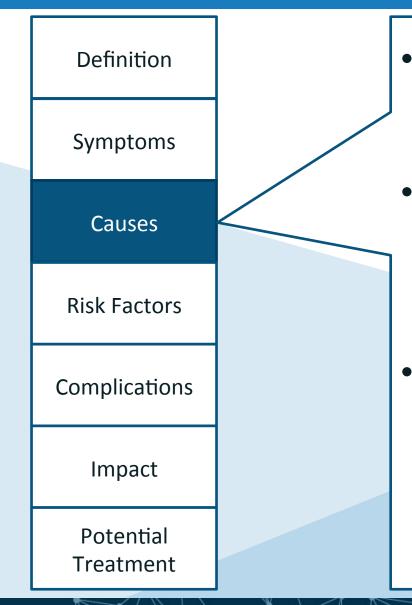
Ø

ICANN

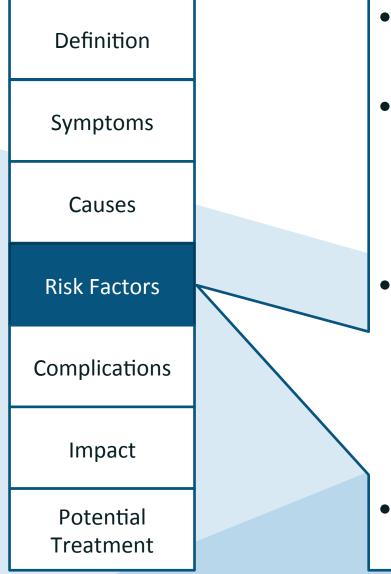
Registrations contain either incomplete, inaccurate or fraudulent data.



- Contact information points to erroneous or non-existing locations or persons
- Large numbers of registrations with similarly incomplete, inaccurate or fraudulent information (often indicative of a spam campaign)

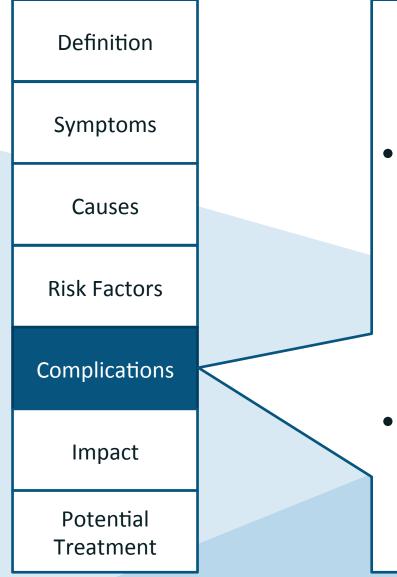


- Some registrants don't supply accurate Whois.
- Out of scope: registrants who use privacy/proxy services
- Registrant/registrar Whois accuracy obligations and registrar verification/ validation obligations not enforced or not consistent.

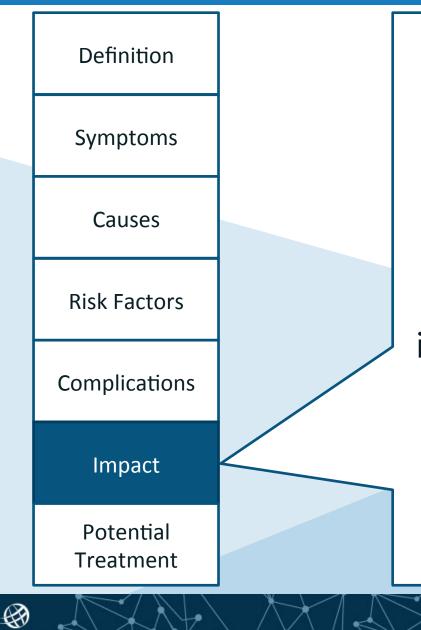


Ð

- Lack of agreed upon definition of accuracy
- Data accuracy/verification/ validation is not enforced (or not enforceable) or not consistent
 National laws may be in conflict with getting access to accurate data (conflict of interest between accuracy
 - and privacy)
- Data may exist but not accessible.

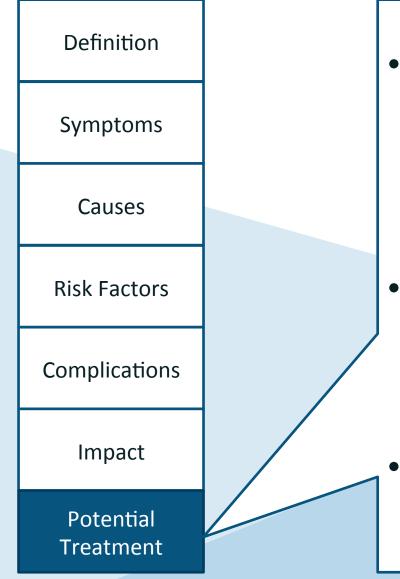


- Registrant fraud:
 - Unauthorized domain name transfers
 - Loss of *contactability*
 - Can escalate to Abusitis



ICANN

Public safety, technical, or business communities have difficulties identifying those responsible for domain names.

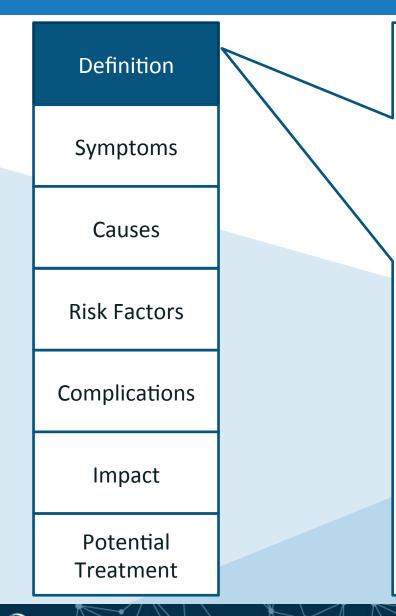


- Contract enforcement: RAA/Registration Agreements, Terms & Conditions
- Acceptable Use Policies that prohibit abuse and misuse of domain names
- National laws may force data accuracy checks

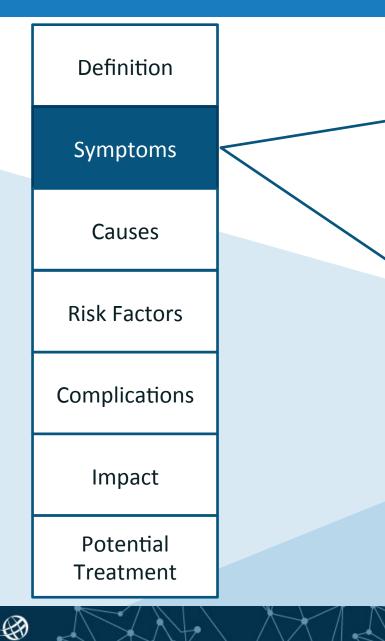
Domain Name Abuse Diseases Abusitis (Abuse Infection)



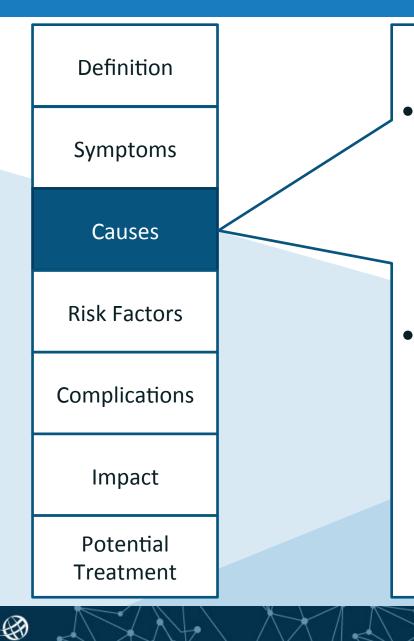




Domain name abuse is the registration or use of a domain name with the capability to cause spam, phishing, malware distribution or command & control of botnets.

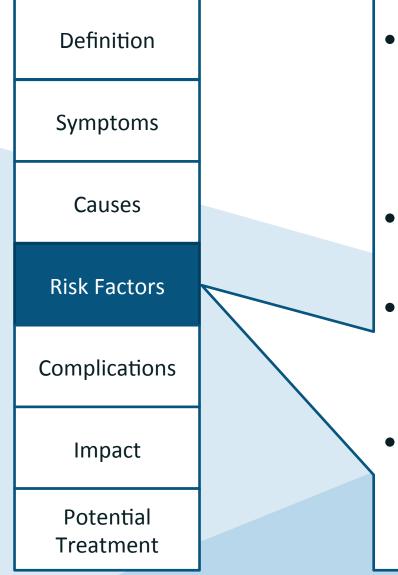


Domain names are involved in spam or phishing, and/or are critical to the use of botnet command & control, and/or in the distribution of malware and other nefarious activities.

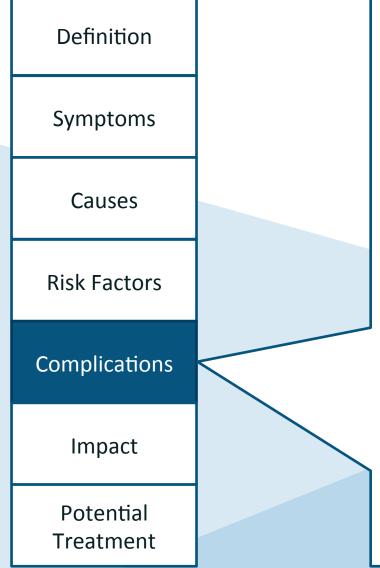


Abusive and/or harmful activities facilitated by the registration and use of domain names.

Contractual & operational
weaknesses or poor
contractual enforcement in
domain name registration
process and life cycle.



- Nefarious intent of the registrant may not be discovered at the time of registration
- Use of privacy/proxy services
 - Incompetent, complacent or complicit behavior of registries/registrars.
 - ICANN compliance department rendered ineffective

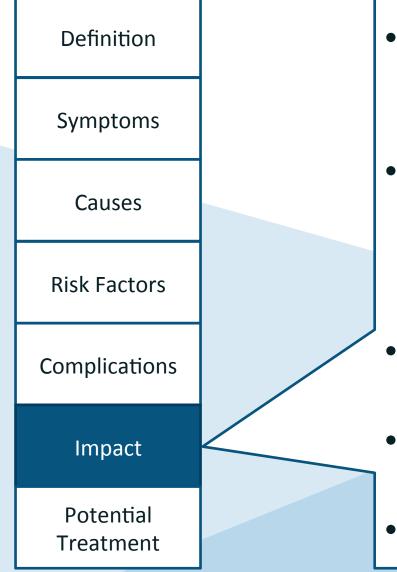


Ð

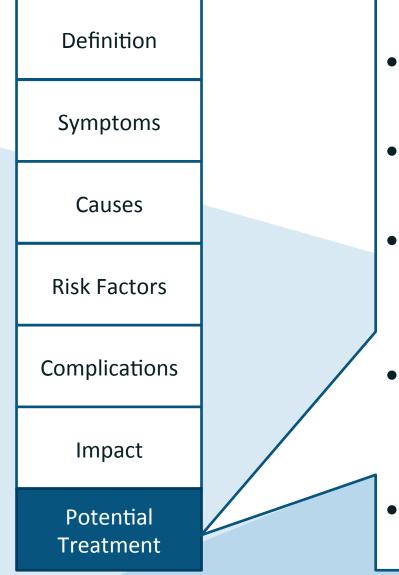
ICANN

Abuse or criminal activities including but not limited to:

- Phishing
- Botnet Command and Control
- Malware Distribution
- Spam



- Domain names associated with abuse may appear in anti-abuse lists.
- Large economical impact for merchants and consumers/damage to brand
- Erosion of consumer confidence
- Erosion of confidence in the DNS system
- Fragmentation of the DNS



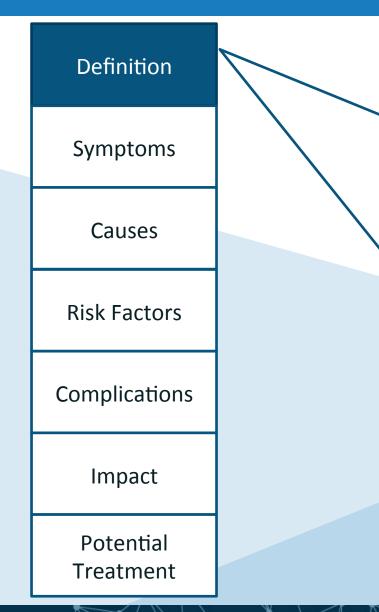
Ð

- Pre-registration automatic screening
- Post registration anti-abuse responses
- Where possible, accelerated procedure for take down
- Common registry/registrar contractual anti-abuse provisions
- Universal minimum price

DNS Server Operation Disease MAGNITUDALGIA (Pain from Quantity)

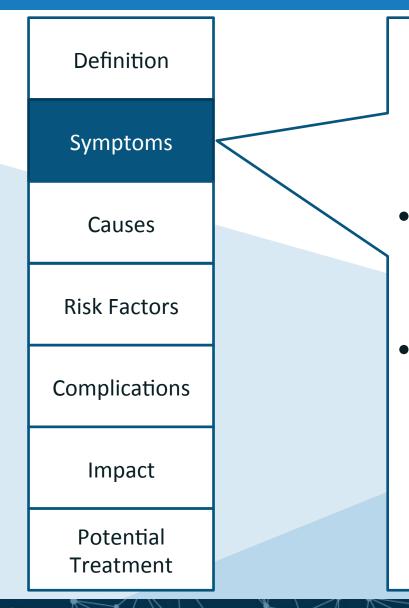






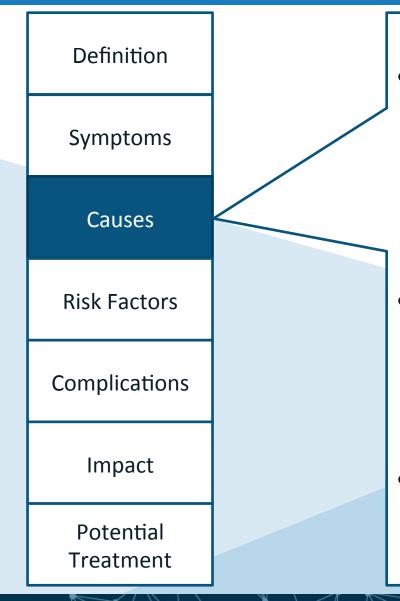
Higher volume of traffic than should be observed in an ideal^{*} world hits DNS servers.

^{*}ideal: no more than a few queries per name per network for the duration of the TTL



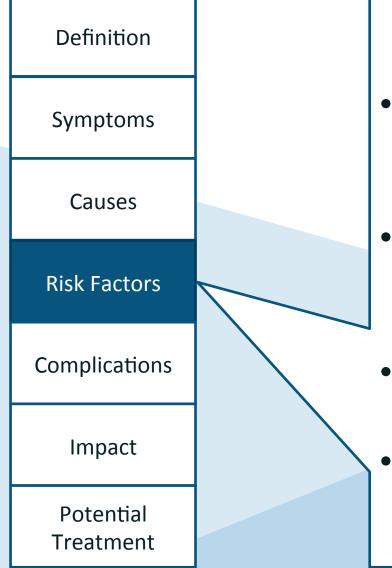
- Monitoring systems detect higher than normal traffic
- DNS servers start dropping traffic.





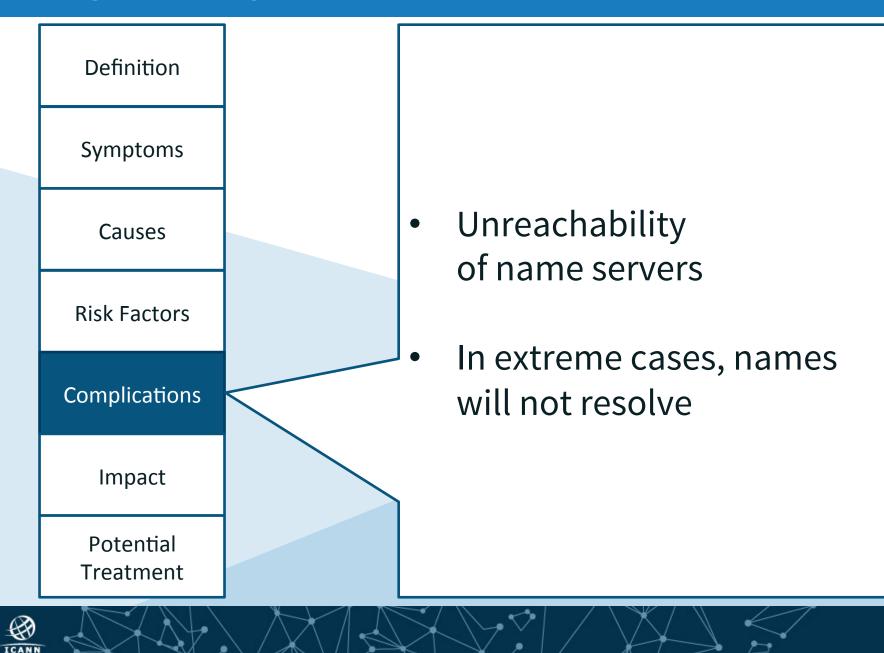
- Many queries are often sent at rapid intervals for the same questions, ignoring TTLs.
- A large number of queries are seen for non-existent names.
- DDOS attacks exacerbate the problem.

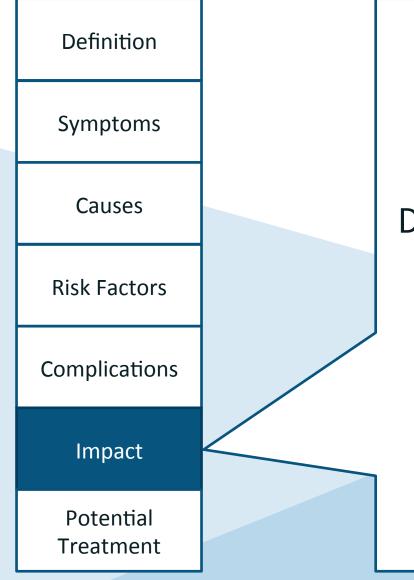




Ð

- Prevalent existence of poorly managed open resolvers
- Proliferation of misconfigured or buggy DNS resolvers
- Lack of deployment of BCP38 (ingress filtering)
- Compromised IoT devices

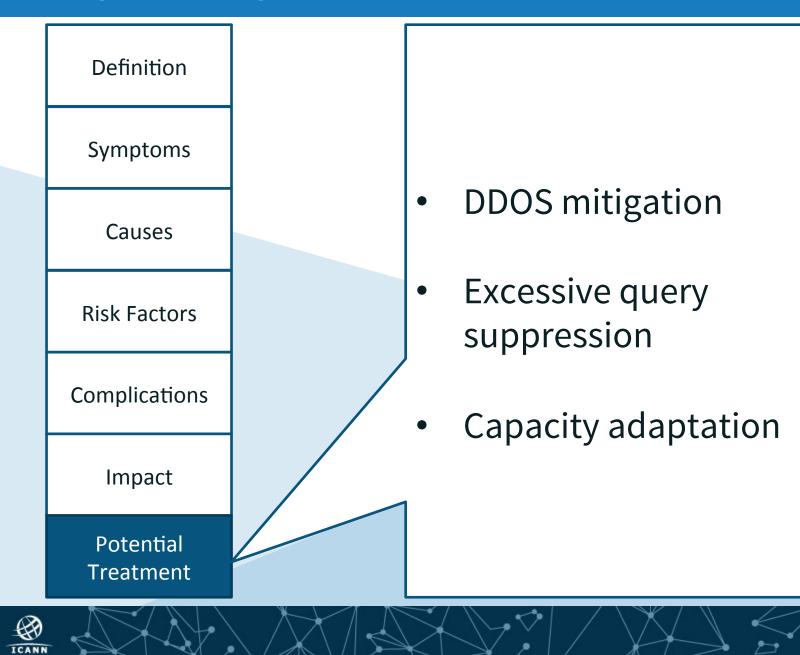




Ð

ICANN

DNS server operators have to build a infrastructure with larger capacity than otherwise.

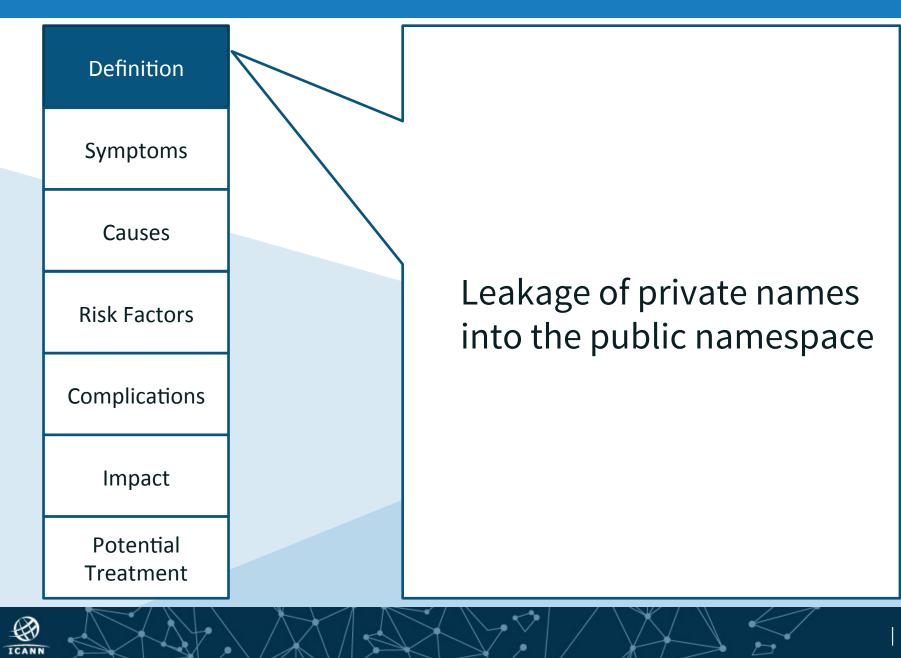


DNS Transmittable Diseases PERFLUOISM (Leakage Condition)

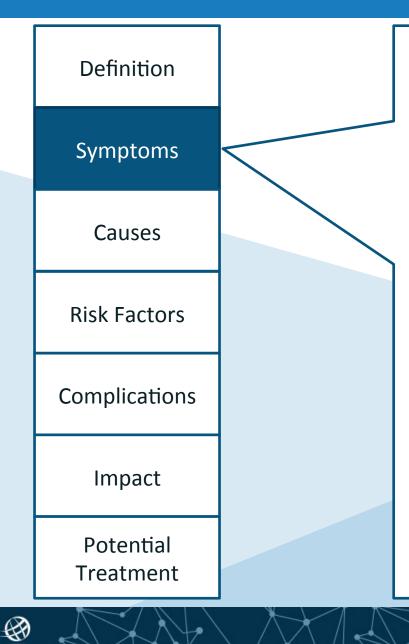




Perfluoism (Leakage Condition)



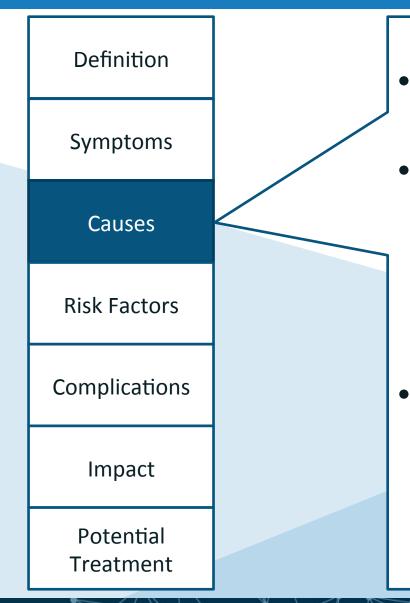
Perfluoism (Leakage Condition)



ICANN

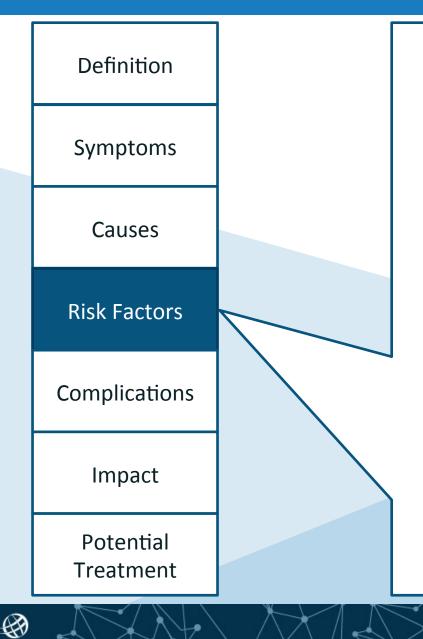
Attempts to resolve private names are observed in the public DNS resolution system

(e.g. .corp, .mail, .home, .wpad, .onion)



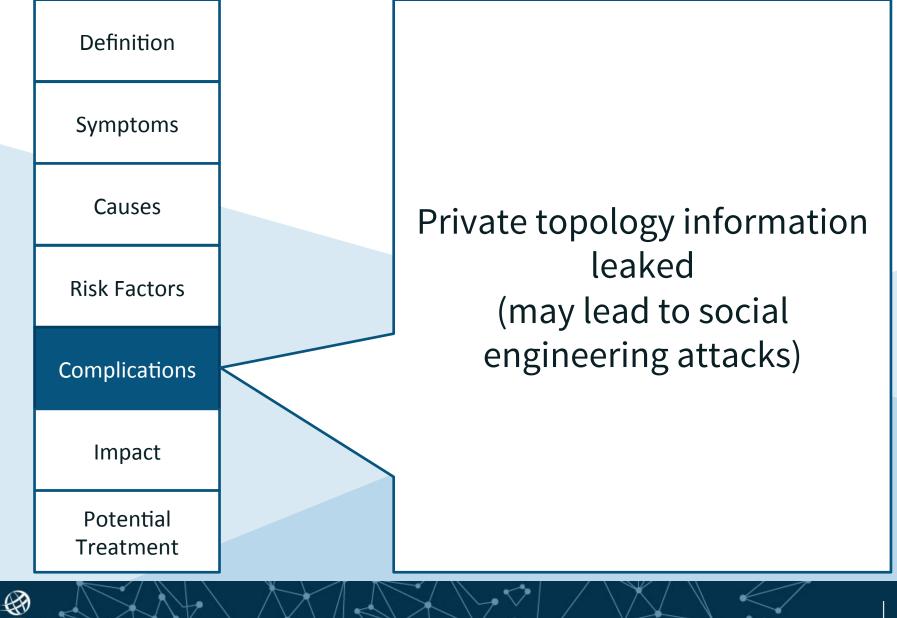
Ð

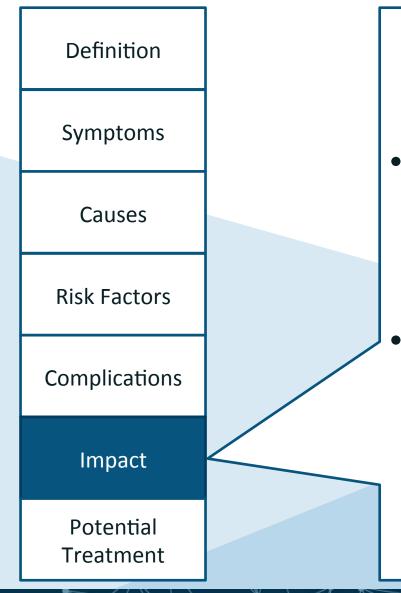
- Misconfigured software
- Poor or inaccurate guidance from vendors regarding use of private TLDs
- "Bring your laptop at home"/connection attempts before VPN is active



- Confusion or lack of awareness of name collision problem
- Unwillingness to change, apathy
- Difficult-to-upgrade (legacy) equipment that embeds private names
- Low cost devices with buggy software using private names

ICANN

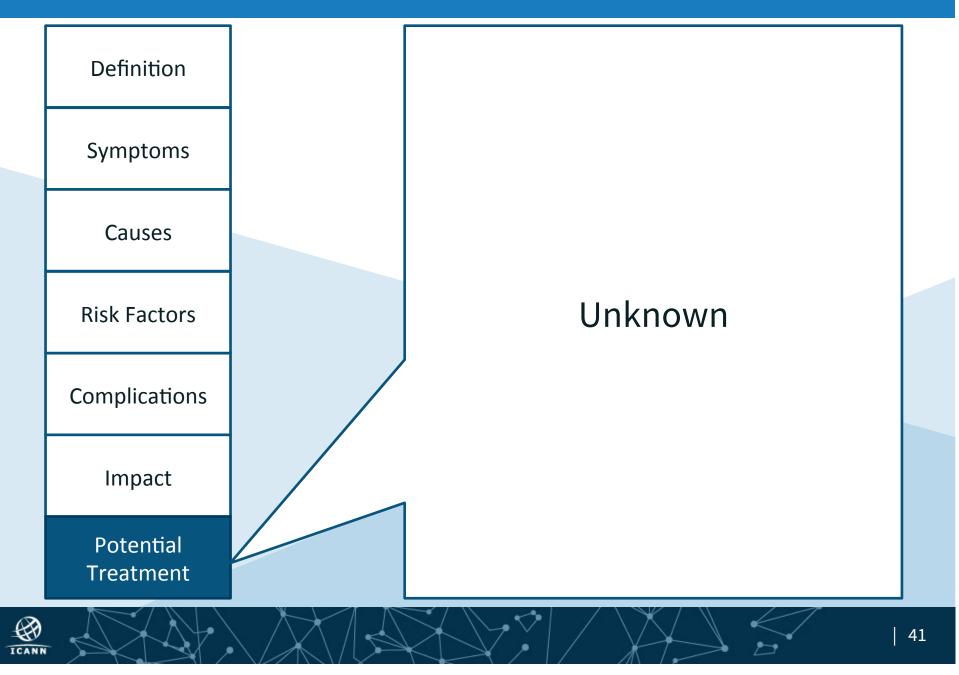




Ð

ICANN

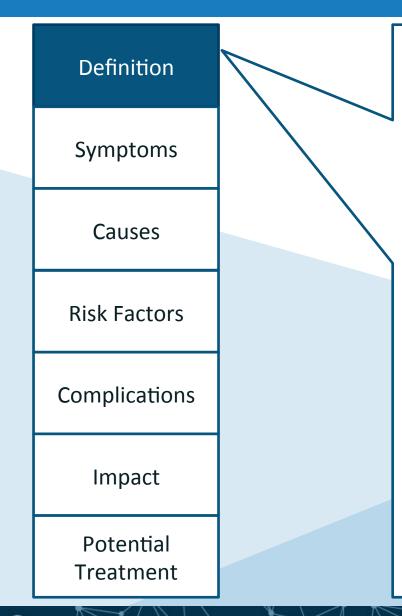
- Privately chosen suffix may become unusable in the global DNS.
- Issue of whether suffix should be made a reserved string



DNS Transmittable Diseases DATAFALLAXOPATHY (Lying Disorder)

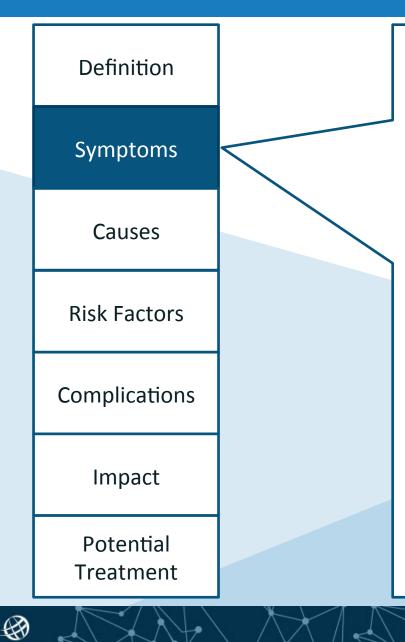






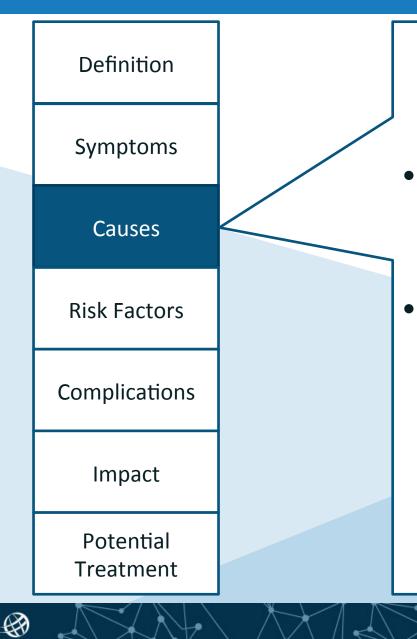
Responses from DNS resolvers to DNS queries contain unauthorized/ forged/tampered data.

Note: This does not include access blocking by regulators or parental control



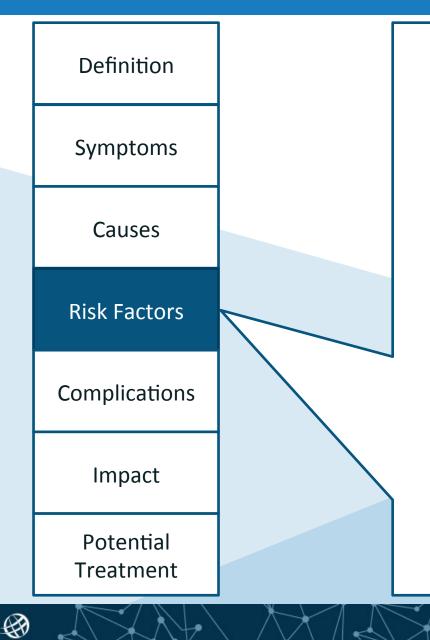
ICAN

URLs are re-directed away from intended servers, e.g., to a competitor, malware distribution, phishing, or defacement site.



ICANN

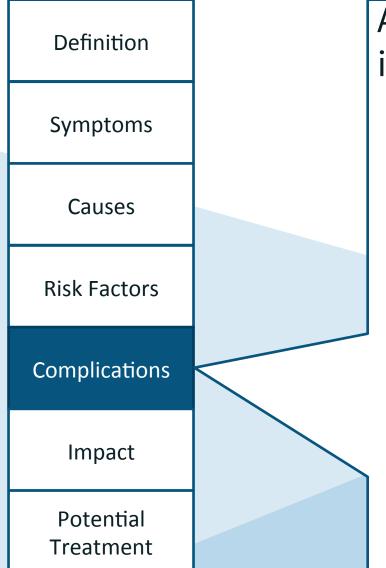
- Cache poisoning or DNS hijacking
- Error resolution service providers (See SAC 032, DNS response modification)



ICANN

Incompetent, Complacent or Complicit ISPs:

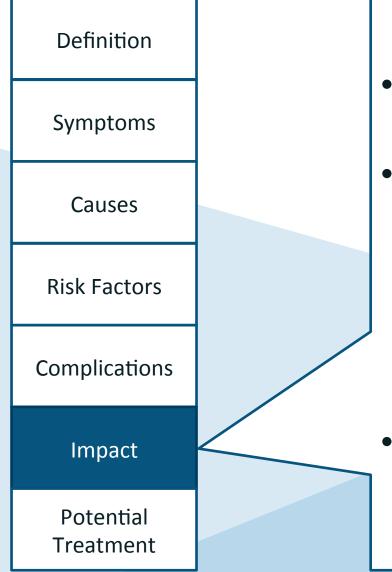
 Services based on name error resolution deployed despite known adverse consequences



Ð

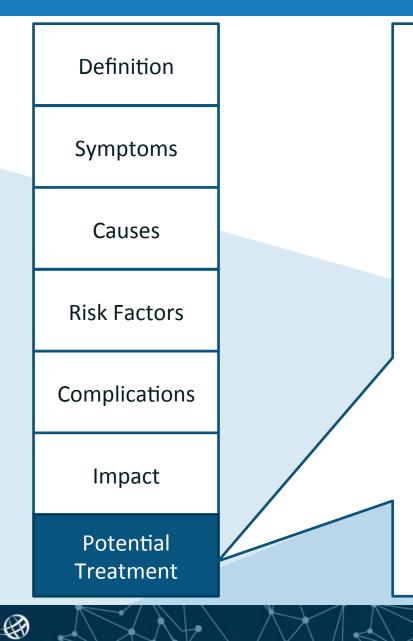
Abuse or criminal activities including but not limited to:

- Malware Distribution
- Phishing, fraud, defacement, hacktivism, DNS or search traffic theft
- Interference with network monitoring or administration (name errors are important to admins!)



Ð

- Loss of business
 - Financial loss (from phishing or from response modification that directs revenue-potential traffic to competitor)
 - Loss of confidence in the DNS system.

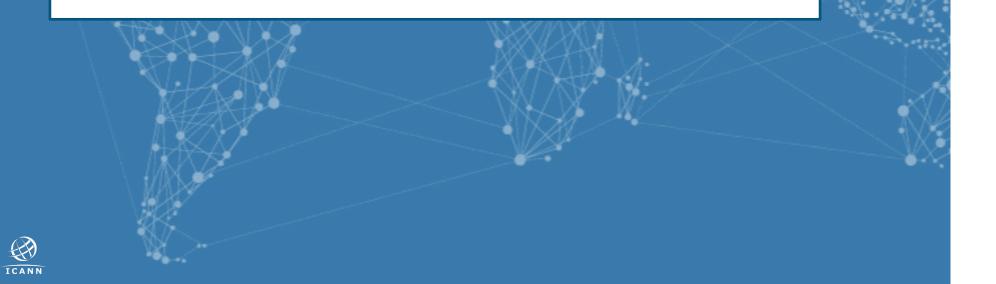


ICAN

Local DNSSEC validation

(indirect effect: if DNSSEC validation was ubiquitous, such attacks would not be possible)

Number Diseases



Number Resource Organization (NRO) update:

"Currently the NRO (trough the Registration Services Coordination Group leadership) is working on the analysis stage for this project, we have identified several steps to complete this work.

During the RSCG face to face meeting which will be held in late November at the AfriNIC meeting, they will review this project definition and work on the risks identification steps (which are the initial parts of the project).

We will share [...] any relevant finding after that meeting"

Oscar Robles, LACNIC CEO, rotating NRO chair. September 30th, 2016

