DNS Abuse and Human Rights	
Individual Right / Freedom	**Relevance to DNS Abuse**
Right to Privacy	**WHOIS:** if the mitigation mechanisms for DNS abuse require disclosure of the domain name holders sensitive and private data such as name, email and mailing address, it might create the risk of privacy violation and human rights abuse. The risk and severity can be measured through: 1) if the registrar is disclosing the data to a law enforcement agency, 2) if the registrar is disclosing the data without receiving much evidence 3) if the law enforcement agency's request can potentially lead to human rights violations
Freedom of Expression (FoE)	**Registrar Duty to Investigate Reports of Abuse and Take Appropriate Action:** The requirement for registrars to "take the appropriate mitigation action(s)" to address DNS abuse is vague and can be interpreted broadly, which could risk leading to the unfair suspension and take-down of the domain names, therefore infringing the domain name holder's right to FoE online.
Right to equal treatment/ non-discrimination	**Protection of rights to fair and equal treatment:** mitigation mechanisms and remedies should be made available in the registrars service region
Freedom of association	**Access to online services that facilitate assemblies:** DNS abuse mitigation mechanisms and processes that could potentially disable a service that provides the opportunity for people to connect and join meetings could have an impact on the right to assembly
Access to Remedy	**In case of take-down or suspension there has to be access to remedy :** If the mitigation mechanisms for DNS abuse prescribe domain name take down and suspension (and even deletion) it is important to provide access to remedy (more specifically a dispute resolution mechanism) for each of the mitigation mechanisms that can go wrong.

Right to a Fair trial / due process of the law	**DNS Abuse mitigation:** Mechanisms for mitigation should afford the domain name holder "due process"

ICANN DNS Abuse Contractual Amendments	
Section 3.18.2 of the RAA	"*When Registrar has actionable evidence that a Registered Name sponsored by Registrar is being used for DNS Abuse, Registrar must promptly take the appropriate mitigation action(s) that are reasonably necessary to stop, or otherwise disrupt, the Registered Name from being used for DNS Abuse. Action(s) may vary depending on the circumstances, taking into account the cause and severity of the harm from the DNS Abuse and the possibility of associated collateral damage.*"
RA: Section 4.2 of Specification 6	*"Where a Registry Operator reasonably determines, based on actionable evidence, that a registered domain name in the TLD is being used for DNS Abuse, Registry Operator must promptly take the appropriate mitigation action(s) that are reasonably necessary to contribute to stopping, or otherwise disrupting, the domain name from being used for DNS Abuse. Such action(s) shall, at a minimum, include: (i) the referral of the domains being used for DNS Abuse, along with relevant evidence, to the sponsoring registrar; or (ii) the taking of direct action by the Registry Operator, where the Registry Operator deems appropriate. Action(s) may vary depending on the circumstances of each case, taking into account the severity of the harm from the DNS Abuse and the possibility of associated collateral damage."*

Relevant Human Rights Instruments	
International treaties / conventions	- Civil and Political Rights (ICCPR, 1966) - Economic, Social, and Cultural Rights (ICESCR, 1966) - Elimination of All Forms of Racial Discrimination (ICERD, 1965) - Elimination of Discrimination against Women (CEDAW, 1979) - Rights of Persons with Disabilities (CRPD, 2006)

International Declarations & Guidelines	- UN Declaration of Human Rights (UDHR, 1948) - Rights of the Child (1923) - Rights of Disabled Persons (1975) - Right to Development (1986) - Cultural diversity (2001) - Rights of indigenous peoples (2007) - Sexual orientation and gender diversity (2008) - The UN Guiding Principles on Business and Human Rights (UNGP, 2011)
Regional instruments	**AFRICA** - African Charter on Human and Peoples' Rights (1981)
	AMERICAS - American Convention on Human Rights (1969) and its Protocols (1988 & 90)
	EUROPE - European Convention on Human Rights (ECHR, 1950) - European Social Charter (1961) and Protocols (1988, 91, & 95) - European Framework Convention for the Protection of National Minorities (1995)

Discussion Questions

- Is this DNS Abuse?
- Are there any human rights impacts? If so, whose human rights are being impacted?
- What human rights are being impacted? What is the severity of impact?
- What are the steps that the registrar should take to follow in order to be in compliance with the contractual amendments and have the lowest impact on human rights?
- Are mitigation actions mechanisms proportional?

Scenario 1

A national oil company's IT service provider has registered the company's domain name (not in the ccTLD space but in the gTLD space). Several of the subdomains are being used for phishing purposes. A law enforcement agency reports the domain name to the registrar and requests for the contact details of the IT services and asks for immediate suspension of the domain.

Scenario 2

A human rights activist owns a domain name and a website through which she shares and documents human rights violations of the country she resides in. A state actor which wants to stop her from raising awareness, takes control of her domain name and through the domain name distributes malware and phishing. The human rights activist's domain name gets taken down.

Scenario 3

A global footwear company named "Yellow Shoes" noticed that a local enterprise that sells sandals, from a country where Yellow Shoes has a registered trademark, has acquired and is using the domain name "mellowshoes.com". The global company reports the domain name to the registrar, classifying it as typosquatting, requesting the contact details of the owner of "mellowshoes.com" and suspension of the domain.

Scenario 4

A brand owner accuses a website, that is being used during a civil protest, of phishing and asks the registrar to take the domain name down. The domain name uses the brand's name to criticize the brand involvement in helping with oppressing people during the civilian protest. However, the website also engages with phishing. The registrar suspends the domain name, the domain name is being used for authentication on other websites and the registrant cannot access the accounts associated until and if the suspension is lifted.