DNS Abuse Institute Roadmap

V1.0 - June, 2021

Version	Changes
1.0	Incorporated inputs and edits
0.9	Initial version of the Roadmap in document form. Adapted from the Roadmap as a slidedeck.

Table of Contents

Introduction

This is the initial Roadmap for the DNS Abuse Institute (DNSAI, or the Institute). The purpose of this document is to provide the reader with clarity on three areas important to the Institute. First, it will discuss the goals of the Institute across the medium and long terms. Second, it lays out the foundational elements the Institute requires to meet those goals, and lastly, it outlines several important building blocks, as well as the Institute's three cornerstone initiatives.

Feedback on this document is welcome, and may be sent directly to graeme@dnsabuseinstitute.org

Misson

The DNSAI has a simple mission: **to reduce DNS Abuse**.

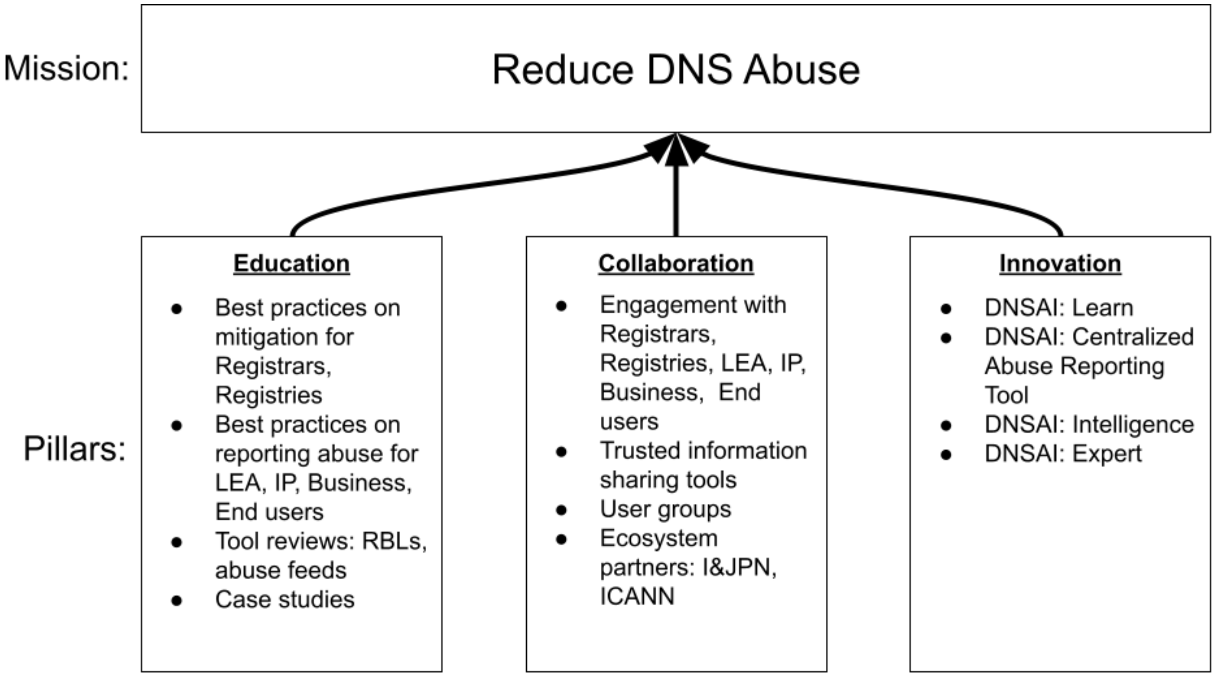
It's possible to add more nuance and specificity to this mission, but to little benefit. The simplicity and clarity of the goal as stated is sufficient to center and guide Institute decision making.

The Institute aims to achieve its mission through three key pillars: Education, Collaboration, and Innovation.

Education: The Institute will develop and distribute guides, primers, best practices, and webinars on DNS Abuse. These resources will be targeted towards Registries and Registrars for mitigating DNS Abuse, as well as towards law enforcement, businesses, intellectual property stakeholders, internet security practitioners, end users, or others experiencing or reporting DNS Abuse.

Collaboration: Collaboration is both a process and an initiative. As the Institute develops resources and tools, it needs to ensure that it's engaged with the communities it seeks to serve and that those communities have opportunities to provide input on the Institute's work. This collaborative and integrated approach is an essential part of Institute working methods. The Institute also needs to provide the tools and opportunities for partners, community members, and new perspectives to work together, share information, and bridge the gaps that currently exist.

Innovation: Innovation will take two primary forms: the first is research and understanding of the DNS Abuse landscape. The Institute needs to have the best data, research, and understanding of DNS Abuse in the ecosystem. It needs to provide definitive analysis, as well as opportunities for others to conduct and contribute to research. The Institute will also need to identify the difficulties in DNS Abuse mitigation and develop tools to address them. These could be tools for the prevention, identification, reporting, or mitigation of DNS Abuse.



Mission: Reduce DNS Abuse

Pillars:

Education

- Best practices on mitigation for Registrars, Registries
- Best practices on reporting abuse for LEA, IP, Business, End users
- Tool reviews: RBLs, abuse feeds
- Case studies

Collaboration

- Engagement with Registrars, Registries, LEA, IP, Business, End users
- Trusted information sharing tools
- User groups
- Ecosystem partners: I&JPN, ICANN

Innovation

- DNSAI: Learn
- DNSAI: Centralized Abuse Reporting Tool
- DNSAI: Intelligence
- DNSAI: Expert

Year Three Goals

We wish to create aggressive but achievable goals for the Institute, which can be used to measure our success. While there will be other initiatives undertaken and goals to accomplish, the following three objectives are what we feel are key to the Institute's success, and against which we think the Institute should be evaluated.

In three years, the DNS Abuse Institute will:

- Be the definitive source for DNS Abuse education and resources
- Be a respected source for DNS Abuse intelligence
- Produce innovations that are widely adopted and valued by the community

We'll address the specifics of each goal in the Cornerstone Initiatives section of this document, as well as the requirements to achieve those targets.

Institute Foundations

This section of the Roadmap outlines the features the Institute needs to develop as an organization, as well as some of the key institutional building blocks required for success.

Advisory Council

DNS Abuse is a complicated global problem, impacting Internet users, businesses, and civil society in a myriad of ways. In order to ensure that the DNS Abuse Institute considers the problem from all appropriate perspectives it will create and fill an Advisory Council to provide insight, guidance, and criticism on Institute projects and initiatives.

The Advisory Council will have up to 12 members, including a PIR Staff Liaison and a liaison to the PIR Board of Directors. The Advisory Council will meet online every quarter to review plans and progress, with the potential for annual in-person meetings.

Member terms will be between 1 and 3 years in order to ensure that the Institute consistently introduces new perspectives and that the entire Council does not turnover at once.

Members of the Advisory Council are expected to participate in three activities where appropriate:

- Provide input and advice on Institute strategy, priorities, and initiatives
- Advocate for the Institute
- Connect the Institute to relevant individuals and organizations

Definition of DNS Abuse

The Institute is focused on addressing DNS Abuse at Registrars and Registries. As such, it uses the definition adopted by the ICANN Contracted Party House:

> *DNS Abuse is comprised of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS Abuse).*[1]

However, the constrained, categorical definition above is not ideal in all cases. For example,there is no easy way of identifying or adding new types of abuse, nor does it offer insight into the attributes of the above harms. So, while there are no plans or interest for the

[1] https://rrsg.org/wp-content/uploads/2020/10/CPH-Definition-of-DNS-Abuse.pdf

Institute in updating or altering the definition, we remain pragmatic in our approach, and attentive to new insights and approaches to defining abuse.

Trust, Transparency, and Security

The work of the Institute has implications for the security of the entire Internet, for the business practices of Registrars and Registries both large and small, and for end-users around the world. Our work is of interest to governments, law enforcement, civil society, registrants, businesses both small and large, intellectual property owners.

Managing these relationships and expectations demands attention and rigor as to how the Institute functions.

Trust

The Institute needs to build and maintain trust with its stakeholders. It will do this through a number of methods. First, it will assiduously identify and protect the information it holds that is sensitive or secret. Second, it will operate with integrity, by stating its intentions and goals, and by meeting its commitments.

Transparency

The Institute will strive to be as transparent as possible. It will have clear and published objectives, as well as concrete plans to achieve those goals. The Institute will share its goals, as well as its assessment of whether they were reached.

Institute initiatives and processes will be publicly available and replicable to the fullest possible extent.

Security

By necessity the Institute's work will include the collection of sensitive information. As well, the Institute’s work may undermine online criminal industries engaged in the operation of botnets, or the distribution of malware. These present substantial security risks, and the irony of having the Institute impacted by malware would be eye-wateringly painful. Consequently, the DNSAI will spend a considerable amount of energy ensuring its systems and initiatives are secure, via audits, tools, and best practices.

Focus on Impact

There are a considerable number of potential activities for the Institute, and it’s clear as we explore the problem space that the scope is extremely broad. Adjacent areas of Internet infrastructure have similar problems. While the Institute should not ignore adjacent opportunities, it needs to remain focused, at least in the short term, on having the greatest impact on DNS Abuse in the least amount of time, requiring the least amount of resources.

The Institute uses the following questions to guide its thinking:

- Will it reduce DNS Abuse?
- Will it help DNS Abuse reporters?
- Will it help Registrars and Registries?
- Will it impact Registrants?
- Will it further our understanding of DNS Abuse?

Approaches for Reducing DNS Abuse

DNS Abuse can be reduced via both preventative and reactive methods. Preventative approaches involve the detection of *potentially* harmful domains as part of the process of registration, and either preventing the registration from completing, or preventing the domain from resolving for some period of time.

Potentially harmful domains can be identified via:

- Attributes of the domain name itself (such as a banking trademark, “-com”)
- Attributes of the registrant, or the customer (links to other harmful domains, payment intelligence)
- Attributes of the transaction (# of domains, payment method)

Proactive methods of DNS Abuse reduction require development and implementation inside of Registrar or Registry domain registration platforms.

Reactive methods depend on the identification of a harmful domain after both registration and malicious activity have occurred. This identification is typically done via two methods: direct abuse reports to the Registrar or Registry, or through a Reputation Block List (RBL) or abuse feed to which the Registrar or Registry subscribes. RBLs and abuse feed providers usually build their data sets through a combination of monitoring, searching, and direct reports of abuse.

Reducing DNS Abuse via reactive methods includes:

- Improving Registrar or Registry response times
- Reducing notification/reporting times
- Eliminating duplicate reports
- Improving notification content/evidence
- Improving Registrar or Registry investigation methods

Reactive methods and tools can often be used by anti-abuse or compliance personnel without requiring integration in the registration platform.

As the DNSAI evaluates initiatives, it needs to consider the implications of the above approaches.

Implementability

The Institute needs to be pragmatic and practical in its approaches to mitigating DNS Abuse. This requires an understanding of not just which approaches would best reduce DNS Abuse, but also which approaches can be feasibly implemented by Registrars and Registries; solutions to DNS Abuse do not exist in a vacuum.

The Registrar market is 21 years old. There are now approximately 2,500 total ICANN-accredited Registrars, belonging to about 425 corporate parents. Approximately 1,730 of those accreditations belong to two different corporate parents engaged in drop-catching, meaning there are about 800 accreditations engaged in the sale of domains.

There are about 28 Registrars with over 1 million domain names registered, and 122 with over 100,000 names. For an industry that generally requires scale, it is a very long tail. As the market matures, Registrars at the top end acquire each other seeking to leverage their size.

The Institute needs to take into account these dynamics in its planning. Many of the larger Registrars are quite old, and many of them operate multiple credentials. This means that Registrars generally concentrate on three things: a) generating revenue, b) maintaining or upgrading aging platforms, and c) integrating acquisitions.

For Registrars, engineering resources are extremely valuable. If the Institute were to focus on primarily developing DNS Abuse mitigation solutions that required extensive implementation by Registrars, then those solutions would need to sit in development backlogs behind business-critical work. There will always be business-critical development work to do. As such, implementation of proactive Institute initiatives will likely be slow, and there will be little to show for some years.

This is why the Institute will focus, at least for the short- to medium-term, on the development of tools and resources that can be employed by Registries and Registrars with minimal development resources. This choice also puts control of the Institute's success back into its own hands rather than being dependent on the resource prioritization of the industry.

Economic Realities

In order to be implemented broadly and therefore make a real impact, Institute initiatives need to reduce the economic impact of DNS Abuse on Registries and Registrars. This impact is felt by the industry in a number of ways, but primarily as costs: mitigating DNS Abuse requires expensive tools as well as trained staff; malicious domains are often registered using fake credit cards, resulting in expensive chargebacks; there is a legal and regulatory cost in maintaining compliance with various obligations.

The Institute needs to provide credible evidence that adopting best practices or using Institute initiatives will not only reduce DNS Abuse, but also that it will reduce the financial burden that comes along with that Abuse. Those costs can be reduced by moving collective issues to individual actors like the Institute.

Both preventative and reactive approaches to DNS Abuse have costs. Over a longer time span, mitigating reported abuse is more costly than preventing abuse before it occurs. However, it's not clear where that crossover in cost lies, partly because preventative action is so development-intensive, and partly because at least some reactive measures will always be required. As such, the Institute approaches the problem by offering least-costly solutions first: education and best practices on preventative and reactive measures, then initiatives to reduce the burdens of reactive mitigation, and then finally the opportunities of preventative mitigation.

Data, Iteration, and Experimentation

The work of the Institute will be measurable, and the choices the Institute makes will be driven by data. Each initiative will have measurable goals, infrastructure to enable that measurement, and a process for reviewing those goals.

Further, Institute initiatives will strive to be incremental and iterative as much as possible. We will learn more, faster, by trying and doing, rather than perfecting.

Relatedly, the Institute needs to understand where an initiative isn't meeting its goals and be unafraid to pivot. If an initiative is not having a meaningful impact, then those resources need to be redirected.

Key Organizational Building Blocks

The Institute requires a number of core competencies in order to be successful. Gaining expertise in these areas will enable the Institute to build useful, impactful resources and tools for the DNS community.The Institute needs to be expert in:

- The various types of DNS Abuse and their attributes
- The different approaches to mitigating and preventing DNS Abuse
- The tools Registries and Registrars both use and need to mitigate abuse

- The attributes, features and qualities of Reputation Block Lists and abuse feeds

Knowledge and expertise in these building blocks are crucial components for the Institute’s initiatives.

Cornerstone Initiatives

The selection and prioritization of initiatives by the Institute was completed by aggregating these principles and ideas into a coherent picture that will reduce DNS Abuse while building Institute capacity and credibility.

In summary, the initiatives selected by the Institute are meant to:

- Reduce DNS Abuse
- Assist Registries, Registrars, abuse reporters, and users of the Internet
- Reflect the Institute’s pillars of collaboration, education, and innovation
- Maximise impact in a minimum amount of time
- Require minimal implementation at Registries and Registrars
- Incentivize Registries and Registrars to adopt Institute initiatives
- Build Institute capacity

DNSAI: Learn

The Learn initiative is meant to fulfill the educational mandate of the Institute. The Institute will produce educational content on a regular, consistent basis, resulting in the best DNS Abuse resource library available.

This content will include:

- Best Practices:
  - For Registries and Registrar to mitigate abuse, both preventatively and reactively
  - For LEA, businesses, intellectual property interests and end users to report abuse, and work with Registrars and Registries
- Reviews and summaries of:
  - Commercial tools for mitigating abuse
  - RBLs and abuse feeds
  - Academic research, industry white papers, and other community efforts
- Webinars and podcasts
- Case studies from within the DNS Industry

The Institute aims to ensure that this content is relevant and useful for the intended audience, and will work with geographic partners to translate and socialize the work.

Initial educational output will be focused on key resources for both the community and the Institute. This will include the review and understanding of useful RBLs, as well as examining current DNS Abuse evidentiary requirements.

DNSAI: Centralized Abuse Reporting Tool (CART)

There are no industry standards on how to implement abuse reporting, what abuse may be reported, and where to report it. As such, there is a substantial amount of variance in abuse reporting methods to Registries and Registrars.

This leads to a number of critical issues. Registries and Registrars receive poorly-evidenced or un-evidenced reports of abuse, often in duplicate, and frequently unactionable. These reports fill queues and require a substantial amount of time and resources to triage but result in little value.

On the other side, stakeholders reporting abuse must identify exactly where and how to address abuse reports, across dozens or even hundreds of Registries and Registrars, each with their own mechanisms and evidence requirements.

To solve these issues, the DNS Abuse Institute will build a centralized abuse reporting tool (CART). At its simplest, the CART needs to have the following functionality:

- Authenticate an abuse reporter
- Accept appropriate evidence for the type of abuse
- Identify the Registrar
- Submit the evidenced abuse complaint to the correct Registrar
- Prevent abuse of the tool itself (submission of malware, bots, spamming the system, ddos etc)

While we believe the benefits from this basic functionality to be substantial, the addition of more features in subsequent versions will make the tool indispensable. These include:

- Customized evidence requirements per Registrar to meet legal requirements
- Enabling communication between reporter and Registrar via CART
- API integration for report submission
- Abuse reporter statistics and reputation
- Enabling Registrars and Registries to embed the forms into their own websites
- Enabling the pass-through of other types of abuse
- Providing a Registrar ticketing system inside of CART

DNSAI: Intelligence

The Institute needs to have a real-time understanding of the DNS Abuse landscape. It cannot rely on others, such as ICANN's DAAR system, for an understanding of what abuse is occuring, when, and where. Perhaps most importantly, in order to be a credible source for information, the Institute needs to be able to publicly demonstrate its understanding and expertise.

As such, and building on the DNSAI: Learn assessment and analysis of RBLs and abuse feeds, the Institute intends to build its own DNS Abuse Intelligence platform. This platform will be similar to DAAR, with some notable differences. The goal is to publish DNS Abuse statics:

- By Registrar, Registry, and TLD
- For ccTLDs as well as gTLDs
- Using *evidenced* data
- That measure persistence, as well as existence
- That distinguish between compromised websites and malicious registrations

There are secondary benefits from this work. The expertise in RBLs and abuse feeds can be shared as part of DNSAI: Learn. DNS abuse trends, insights, and intelligence can be shared with Registries and Registrars. There is the potential to link the DSNAI: CART to the DNSAI: Intelligence and derive trends and insights from what's being manually reported.

The intent of the Institute is to measure the abuse that could reasonably be acted upon, and to assess the speed at which that action takes place. The Institute also intends to publish the methodology for how it measures DNS abuse, so that the process is transparent, credible, and reproducible by any interested stakeholder.

Secondary Initiatives

DNSAI: Expert

The DNSAI: Expert initiative is a DNS Abuse referral service for Registries and Registrars. Where Registries and Registrars encounter suspected or complicated DNS Abuse outside their expertise, they can refer it to the Institute for analysis and suggested actions. The goal with this initiative is to support the industry as much as possible in its efforts to mitigate abuse, while building Institute capacity.

This function was quietly launched with the Institute's creation, with referral submission via supportline@dnsabuseinstitute.org. The Institute plans to expand this offering by making it more accessible and increasing awareness among Registries and Registrars.

DNSAI: Share

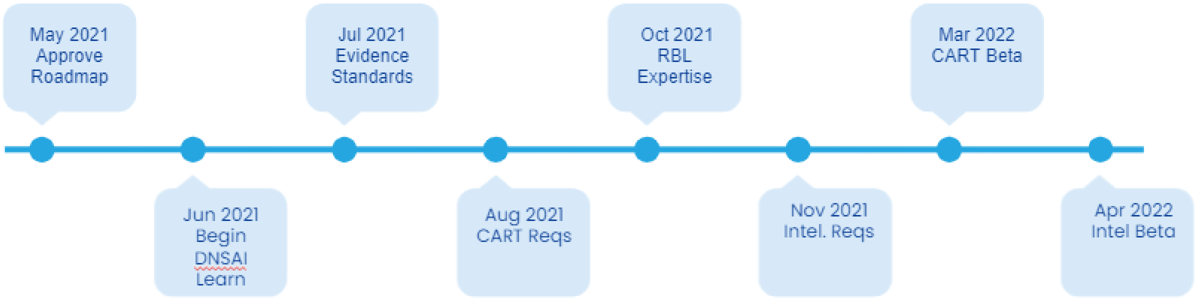
Registrars and Registries do not currently have a dedicated, trusted platform for sharing information related to DNS Abuse. While there are a number of adjacent spaces, the Institute wants to ensure that those who have the power to mitigate DNS Abuse have a place to share intelligence, threats, processes, and best practices. The sensitivity of some of this material makes the platform choice, and who has access, important.

The Institute is exploring its ability to leverage existing trusted spaces, as well as establishing its own to support this collaborative function.

Timeline

Work to build detailed project plans for DNSAI: CART and DNSAI: Intelligence is already underway, as well as prioritization of output under DNSAI: Learn. There are two key foundational pieces of work that will support all of the above initiatives: a) consuming, understanding, and analyzing the various relevant RBLs and abuse feeds, and b) establishing the minimum evidentiary requirements standards for reporting each category of abuse. Resources and infrastructure to support those efforts are also already being put in place.

Until more detailed project plans have been finalized, the timeline below is speculative. The Institute will both publish project plans and accept public input on them.



What's Next

This roadmap provides a reasonably ambitious set of goals and initiatives for the short and medium term. While we hope to have a substantial impact on DNS Abuse within that period, there will be more work to do.

Iteration

The Institute has selected initiatives with substantial room for growth and iteration. The Learn, CART, and Intelligence initiatives will benefit from new features and consistent development over the longer term. As well, the Institute needs to ensure that it keeps pace with Industry needs and the changing DNS Abuse landscape. The Institute's focus on experimentation, iteration, and data driven decision making will ensure that these efforts grow in appropriate ways, and remain relevant.

Prevention

While the Institute intends to produce educational and best-practice content related to preventive measures, none of the above Initiatives approach DNS Abuse mitigation in this way. The next reasonable step for the Institute is to investigate what preventative measures can and should be implemented by Registries and Registrars, and how the Institute can support those efforts.

There are interesting efforts underway using machine learning to identify malicious domains at the time of registrations, as well to distinguish between malicious domains and compromised websites. Helping these efforts mature, as well as providing mechanisms for easy integration is of substantial interest to the Institute.

Further, developing the best practices around preventative measures will be fruitful work. Applying an appropriate amount of friction in the registration process, proportionate to the perceived risk of the domain(s) is delicate work and requires careful consideration. It is rare within the industry to acknowledge that the perceived risk of a domain isn't binary but falls along a scale, and that there are potential actions which can be taken along that scale. We look forward to tackling these challenges.

Structure

PIR created the Institute in furtherance of its 501(c)(3) nonprofit mission. It did so in order to benefit the Community by enabling it to better identify and address DNS Abuse. For the immediate future, the Institute will focus on the projects described in this Roadmap. After we've tackled some of these problems and implemented some solutions, we may revisit the model of the Institute being a part of PIR directly, but for now we're rolling up our sleeves and focusing on getting the work done.