Controlled Interruption
(aka “what we did last time”)
vs.
Controlled Exfiltration
(aka “Honeypot”)

Cost-Benefit Analysis (1)

	Controlled Interruption	Controlled Exfiltration (aka Honeypot)
Notification Experience	Requires “decoding” 127.0.53.53 Largely uniform across all protocols/logs: IP is easy to search for, single-purpose, attracts attention, won’t change Triggers failure for all protocols – breaks most things to draw attention (if no local service attached, will return RESET from all modern IP stacks, by design)	HTTP[S] superior client notification (informational web page) Other protocols/logs: no well-known IP just some unremarkable public IP that won’t be as “known” as 127.0.53.53. May change, may be multi-purpose, certainly not as obvious to trigger inquiry. May not trigger failure where honeypot services are provided (connection will be established, unknown things happen from there)

Cost-Benefit Analysis (2)

	Controlled Interruption	Controlled Exfiltration (aka Honeypot)
Can be blocked at firewall, logged, redirected, etc., by sophisticated enterprises and ISPs	In most cases yes, by rewriting DNS responses	In most cases yes, by rewriting DNS responses and/or by leveraging the known public IP
Directly applicable to IPv6	Possible but would require modification that is not straightforward. On the plus side, IPv6 implementations have become more predictable and robust than they were in 2014.	Yes

Cost-Benefit Analysis (3)

	Controlled Interruption	Controlled Exfiltration (aka Honeypot)
Centralized Data Collection	By design there is no centralized collection of data	Honeypot operator would have the ability to collect vast amounts of data from systems experiencing collisions issues Honeypot operator possesses a long-lived list of vulnerable/misconfigured hosts Honeypot operator has all the obligations and liabilities of holding such data

Cost-Benefit Analysis (4)

	Controlled Interruption	Controlled Exfiltration (aka Honeypot)
Measurement of Performance (Improvement attributable to notification mechanism)	Performance is not directly measurable. Performance is measured through second-order artifacts (e.g., posts to technical support fora). Second order artifacts are more resistant to gaming. Does not directly provide data for additional research	Performance may be directly measurable via metrics collected at the honeypot. However, those metrics are subject to gaming and may be unreliable for intended purpose. Directly provides data for additional research
Ongoing data management obligation	None	Creates data lifecycle obligation to mange, control access, vet researchers, vet projects, sanitize data, etc.

Cost-Benefit Analysis (5)

	Controlled Interruption	Controlled Exfiltration (aka Honeypot)
Direct impact on security posture of the target host	None. Host is no more or no less secure than they were without CI	Reduced security posture. Host is arguably less secure than they were without the honeypot
Host data (possibly sensitive) transmitted over the Internet	None. Use of 127/8 assures that data will not leave the host	Yes. Use of public IP assures that data will leave the host and be transmitted over the Internet, possibly unencrypted

Cost-Benefit Analysis (6)

	Controlled Interruption	Controlled Exfiltration (aka Honeypot)
Privacy regulation impact	None. No data is requested, transmitted, caused to be transmitted, or stored.	Honeypot causes data, possibly sensitive data, to be sent to and possibly stored at the honeypot. Under GDPR and similar frameworks, ICANN would likely become a "Data Controller" by *determining the purposes and means of the processing of data* The Honeypot Operator would likely become a "Data Processor" which *stores and processes data on behalf of the controller* *(not a lawyer, not legal advice)*

Cost-Benefit Analysis (7)

	Controlled Interruption	Controlled Exfiltration (aka Honeypot)
Involvement of additional parties	None	ICANN would need to contract with one or more honeypot operators
Root zone changes	As currently specified (CI run by new Registry), CI adds no additional root zone changes	At least 2 additional changes (delegation to and away from honeypot operator, depending on exact implementation)
Total Cost	None	High

Yes, but there's lots of other honeypots…

- Honeypots are not new and quite a few exist in the security research world. The contemplated collision honeypot is very different.

- Other honeypot projects create interaction with folks suspected in Good Faith of being bad actors or traffic generated by malware. A collision honeypot would interact with good actors. Many of those good actors are commercial entities. Many of those commercial entities have lawyers.

- Other honeypot projects are passive: they respond to unsolicited inbound requests, they do not technically cause/solicit traffic to be sent that would otherwise not be sent.

- A collisions honeypot would be created with the a-priori knowledge that it would cause the sensitive information of good actors to be transmitted over the Internet. As Google said: *"Unfortunately, some protocols will send sensitive information unsolicited (e.g., login.example/login.php?user=fred and HTTP cookies). The honeypot will specifically not log this sort of information, but this doesn't change the fact that the information has been communicated over the Internet."*

Yes, but SSAC recommended a honeypot… (1)

- Actually, no. SAC066 Recommendation 3 merely suggests ICANN “perform an evaluation of potential notification approaches…”
- SAC066 overstates the HTTP[S] notification benefits of a honeypot over 127/8 (honeypot notification is marginally superior in the limited HTTP[S] case)
- SAC066 understates the non-HTTP[S] notification benefits of 127/8 over a honeypot (127/8 notification is marginally superior in the non-HTTP[S] cases)
- In 2014, SSAC could not have been aware of the “equity” now present in 127.0.53.53. Back then it was just a funny IP. Now it has meaning which makes it valuable for this purpose. Searching for “127.0.53.53” yields relevant/valuable front page search results in all search engines.
- SAC066 incorrectly values “(1) Communication” and “(2) Measurability” over “(3) Minimum Harm.” “Minimum Harm” must be the primary consideration.

Yes, but SSAC recommended a honeypot… (2)

- SAC066 minimizes the material risks concerning “privacy” and “information leakage”
- SAC066 does not recognize the material differences between honeypots run for security research and those contemplated for this application (previous slide)
- SAC066 is silent on the costs of a honeypot provides no cost-benefit justification of the increased costs over 127/8
- SAC066 is silent on the reality that centralized data is vulnerable to gaming by future applicants and may be unreliable for intended purpose
- SAC066 is silent on the regulatory obligations and risks of a honeypot. Global privacy regulation has evolved dramatically since SAC066 was written in 2014.