Federal Register Notice 88 FR 7999, Federal Register: Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan, March 3rd, 2023

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

David Clark

Kc Claffy

Subject: RFI Response: Federal Cybersecurity R&D Strategic Plan
Date: 3 March 2023
From: kc claffy CAIDA, UCSD, David Clark, CSAIL MIT

We write in response to the above-cited request for information. Our response draws on our collective history of research in Internet measurement, Internet security, and the relation of technical innovation to the larger societal context in which the Internet is positioned today.

Focus on Internet security

We urge that the R&D Strategic Plan be explicit in giving priority to the security of the Internet itself. The introduction to the 2019 plan mentions security of the Internet several times, but the rest of the report mentions it only once (aside from the phrase Internet of Things) in Trustworthy Distributed Digital Infrastructure, and there in the subsection on 5G and Post-5G. That section talks about the "accelerated development and rollout of next-generation telecommunications and information infrastructure". The report thus elides an underappreciated fact: society must live with the current-generation Internet we have today. Improving the security of the current Internet may not seem innovative, but it is critical. We note that the 2019 report refers to "seamless, end-to-end security across interconnected networks with multiple owners, trust domains, …" We agree that this is the correct scope of the critical challenge, but urge that it not be equated to "next-generation".

We understand that the focus on the Strategic Plan is on research priorities, not preferred research outcomes. However, we believe that better security of the Internet will require a reconception of how to approach the problem. The challenge is often stated using phrases such as: "improve the global security of the Internet". But thus stated, the goal is intractable because at that scale, the Internet includes malicious actors inside the system. We must adjust, and think about how to secure regions of the Internet (what we call *zones of trust*), or classes of user behavior (design of applications that damp abusive activities) knowing that we cannot exclude malicious actors from the ecosystem.

The report would benefit from articulating the specific vulnerabilities at the Internet layer: Distributed Denial of Service attacks, abuse (often in the context of DDoS) of the source address in packets, malicious routing announcements, vulnerabilities and abuse of the DNS and the Certificate Authority system. By flagging the specific vulnerabilities, their implications become more tangible.

Improving the trustworthy character of the user experience.

The section on Distributed Digital Infrastructure uses the word "Trustworthy" rather than "Secure" in the heading. We encourage a continued focus on making the Internet experience trustworthy, and note that a ``secure system'' (in its formal sense—that it operates according to its specification even under attack) does not automatically produce a safe or trustworthy experience. Much abuse on the Internet today, ranging from phishing to disinformation, is exploiting the features of the Internet as they were designed to be used.

However, most subsections of that section (and R&D goals) focus on technical innovations more related to security, rather than making the user experience more trustworthy. We urge elaboration of the challenge stated in the introduction: "to elevate human-oriented issues to be among the priorities for cybersecurity R&D".

The report has a strong section on privacy, but privacy is not the only, or perhaps not the most important, aspect of making the online experience more trustworthy. We support the mention in the section of Critical Dependencies of social and behavioral studies, and developing psychological, sociological and economic models. We urge that the report not view security as a primarily technical problem.

Enabling academic research on Internet security

In the section on Implementing the Plan, (the subsection on Academia and Research Organization), the report states that "researchers should provide comparisons against open datasets". This passing mention of open datasets does not address the larger challenge here, which is much of the data that will enable academia to participate in security research (and Internet research more generally) is collected by private-sector firms and is considered proprietary. Governments need to address the challenge of getting data about the operation of the Internet into the hands of the research community. This is critical for workforce development as well as sustaining the role of academia in understanding and improving cybersecurity.

The issue of access to data will evolve as the government takes more interest in the character of the Internet, and possible roles for regulation. The government will also collect data to support *its* role. A starting assumption might be that industry-provided data is available only to the government, protected by data sharing agreements with industry. We urge that this not be the norm. The European Union, in a regulatory context (which we understand is different from the space within which NITRD operates) has clearly articulated that independent academic research must be sustained by access to relevant data.

In their proposed regulation for Digital Services[1] they discuss the importance of ensuring access to proprietary data by the academic research community. The report states:

> *Investigations by researchers on the evolution and severity of online systemic risks are particularly important for bridging information asymmetries and establishing a resilient system of risk mitigation, informing online platforms, Digital Services Coordinators, other competent authorities, the Commission and the public. This Regulation therefore provides a framework for compelling access to data from very large online platforms to vetted researchers.*

They clarify what they mean by "vetted researchers":

> *In order to be vetted, researchers shall be affiliated with academic institutions, be independent from commercial interests, have proven records of expertise in the fields related to the risks investigated or related research methodologies, and shall commit and be in a capacity to preserve the specific data security and confidentiality requirements corresponding to each request.*

This regulation emphasizes a structure that allows the academic community to work with proprietary data, sending an important signal that they intend to make their academic research establishment a recognized part of shaping the future of the Internet in the EU. The U.S. needs to take a similar proactive stance, and we encourage NITRD to advocate for this stance.

Deterrence

The 2019 report states that "Deterrence also requires successful attribution of cyber attacks to specific offenders to dissuade them from pursuing cyber attacks." We believe that raising the level of effort that attackers must expend need not depend on attribution, and given the global nature of the Internet, as you note, we would urge an emphasis on other dimensions of deterrence—in particular, new design principles for applications that raise the cost of abusive behavior. In our view, the emphasis on forensic analysis may be misguided, and if this sort of attribution is important, it will be of most relevance at the application layer. This point is important, in that it brings a focus on the correct layer of the ecosystem.

---

[1] European Commission", "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services," 2020. https://eur-lex.europa.eu/legal-content/.