CDNs & States

Nick Merrill
University of California, Berkeley
Center for Long-Term Cybersecurity

Look ma, no Tier-1!

- As a percentage of internet traffic...
  - Google: 21%
  - Netflix: 9%
  - Meta: 15%
  - Akamai: 15-20%
- Most internet traffic comes from offnets!
- Though its death is overhyped, the Tier-1 network is much less relevant than it used to be.
  - ...though policymakers don't know that yet (Merrill & Narechania, 2022)

So... how do states think about CDNs?

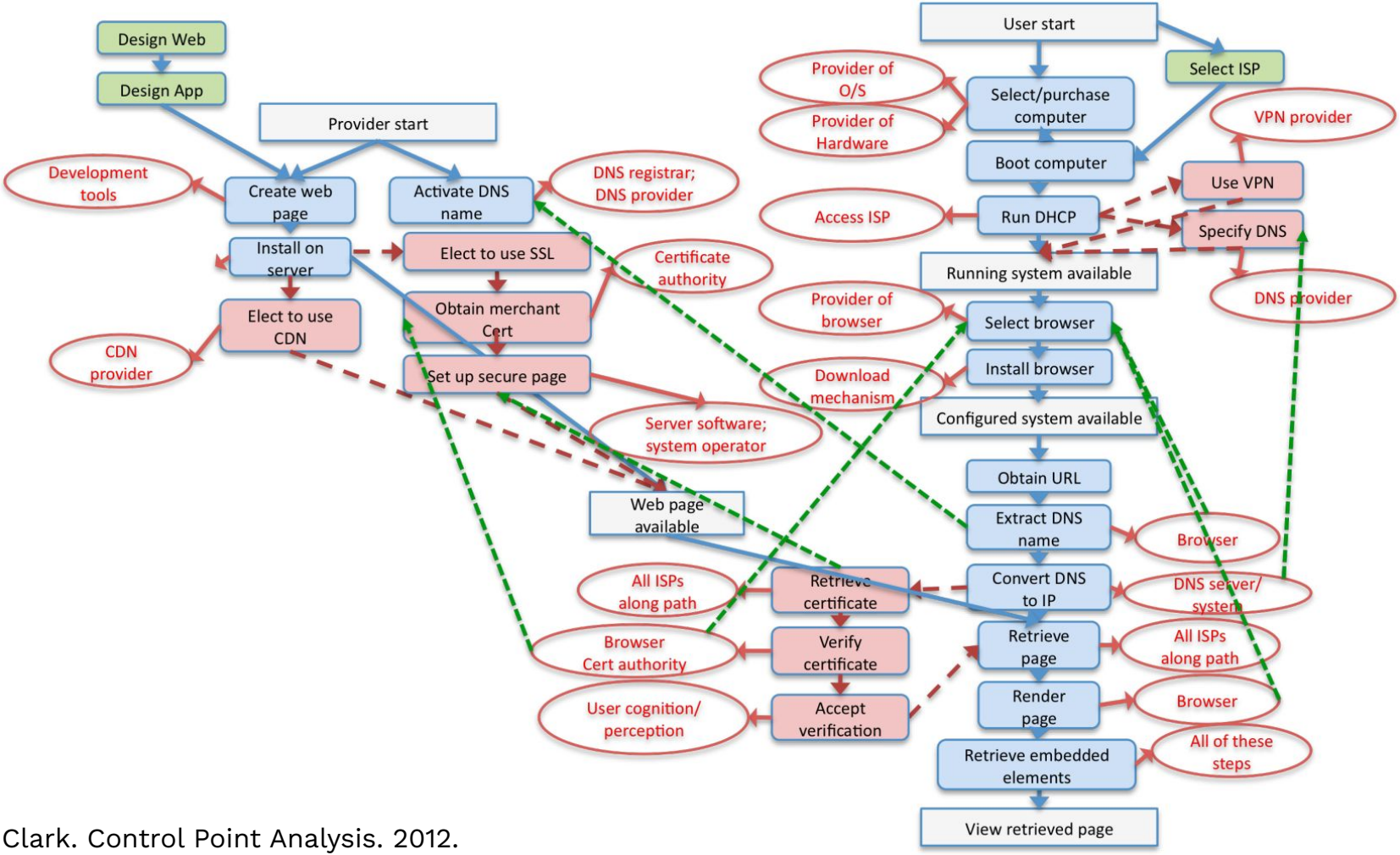
- The internet is both the cause and effect of geopolitics (Douzet, 2014).
  - China's "Great Bottleneck" (Zhu et al., 2020)
  - Iran's selective international censorship (Salmation et al., 2021)
  - Eastern Ukraine's dependency on Russia (Limonier et al., 2021)
- How do CDNs fit into this picture?

Narrowing the question

1. How do states want the internet to be (and why)?
2. How do CDNs want the internet to be (and why)?

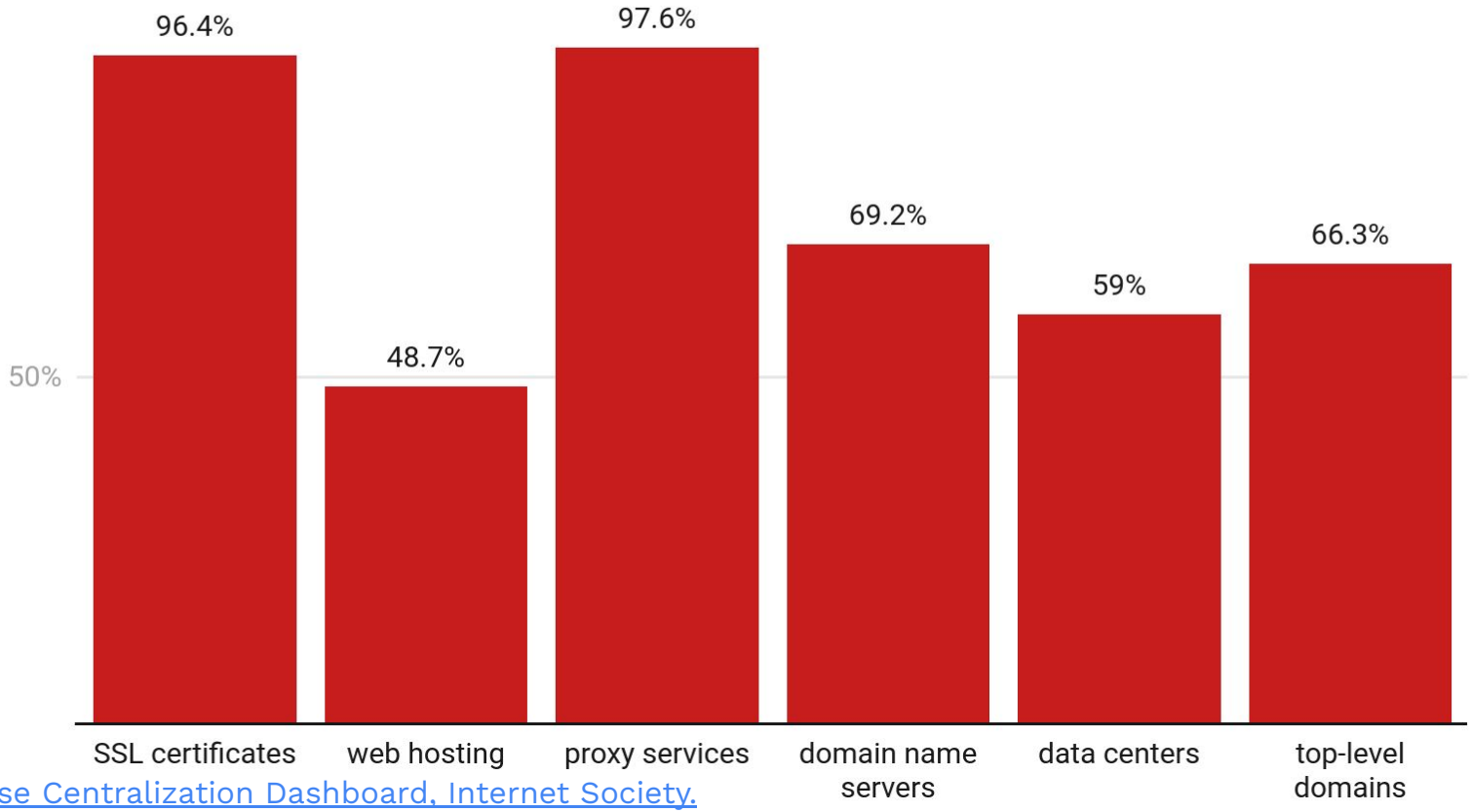
We know a good amount about (1), but less about (2), and almost nothing about the relationship between 1 and 2.

Why care?



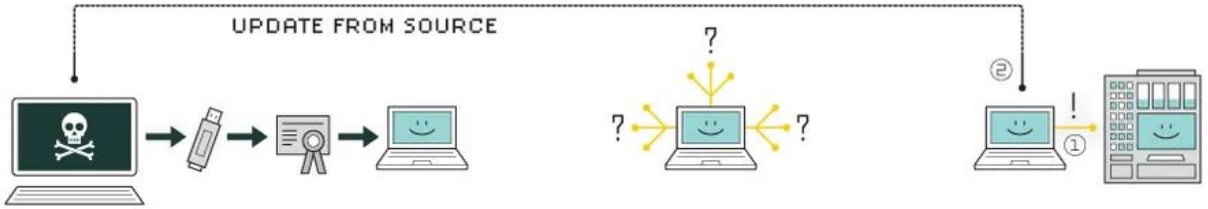
David Clark. Control Point Analysis. 2012.

The proportion of core internet services provided by U.S.-based companies by marketshare.



Merrill, Pulse Centralization Dashboard, Internet Society.

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Source: IEEE Spectrum.

A research agenda

- Understand CDNS' decision-making from IETF mailing list data
  a. Decision-Dialogue-Act Analysis on IETF datasets (Karan et al., 2023)
  b. ten Oever, N., Milan, S., & Beraldo, D. (2020). Studying Discourse in Internet Governance through Mailing-list Analysis. In D. L. Cogburn, L. DeNardis, N. S. Levinson, & F. Musiani (Eds.), Research Methods in Internet Governance. Cambridge, MA: MIT Press.
- Compare those findings with best-available information about state desires
  a. U.S. agencies?
     i. State Department DRL?
  b. E.U. agencies?
     i. ???
  c. Others?
     i. ????
- Understand points of (1) alignment (2) friction