13 Propositions on an Internet for a "Burning World"

Tobias Fiebig
Max-Planck-Institut für Informatik
tfiebig@mpi-inf.mpg.de

Doris Aschenbrenner
Aalen University
Doris.Aschenbrenner@hs-aalen.de

ABSTRACT

In this paper, we outline thirteen propositions on the state of the Internet and digital infrastructures. The core of our theses is that the centralizing Internet of today will not be sustainable and resilient, neither in terms of its energy needs nor in the face of a "burning world", i.e., the rapidly changing world, facing an unprecedented human-made climate disaster and countless other shifts we currently find ourselves living in. Furthermore, we highlight that ongoing policy decisions do not necessarily benefit the resilience of the Internet in the future to come. Our propositions are based on our own research contributions published in the past, public discourse, and most certainly rooted in system administration lore and our own experience as system administrators. They are intentionally bold, to form a foundation for discussion, and we make no personal claim to originality and completeness. Finally, we note that, they do not aim at providing simple solutions, but hint at interrelations and challenges we *must* resolve to survive the future to come.

CCS CONCEPTS

• **Social and professional topics → Computing industry**; **Management of computing and information systems**; **Computing profession**; **Computing / technology policy**.

ACM Reference Format:
Tobias Fiebig and Doris Aschenbrenner. 2022. 13 Propositions on an Internet for a "Burning World". In *Proceedings of ACM SIGCOMM Workshops TAURIN+BGI'22.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 PROPOSITIONS

Proposition 1

> *Operating systems requires operators to execute care, towards their system, their users, and the infrastructure as a whole.*

As Kaur et al. [16] describe, system administration has a major component of care work and emotional labor. This aspect alone should be self-evident to any system administrator who ever had a user ask them if they happened to have 'a backup' of something important the user lost. Maintaining the user's emotions, fear, and anxiety, regardless of whether a backup is present, is the major part of the task.

ACM SIGCOMM Workshops TAURIN+BGI'22, August 22 / 26, 2022, Amsterdam, The Netherlands

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM.
https://doi.org/10.1145/nnnnnnn.nnnnnnn

However, we also claim that the necessity to care for users extends beyond this example. To operate systems means *caring* to create those backups in the first place. System administrators need to plan in advance, anticipating needs, and provide solutions for problems before they materialize and are realized by users.

Furthermore, system administration means caring for systems in their whole life cycle. While building a system is fun, ensuring that it keeps running is a different and more complex task—especially under the security and privacy guarantees users expect. Following, e.g., the gist of Limoncelli et al.'s book on system administration [19], providing a service is a responsibility that has to be fulfilled, and the *hard* part is *continuing* to fulfill it.

Proposition 2

> *The centralization of the Internet has been promoted by a lack of care.*

The early Internet used to be a rather collaborative network, and that also showed in the protocols that were developed for it [11]. Initial visions for SMTP (open relays being the default) or DNS (neglecting the issue of spoofing) serve as examples of how paradigms turned from useful to dangerous. Especially the abuse of DNS gave rise to large-scale Denial-of-Serivce (DoS) attacks [28].

The prevalence of high-bandwidth DoS attacks essentially made it impossible to *reliably* run a service that is not shielded by the *'just having a bigger pipe'* of a hypergiant (like Cloudflare, Amazon or Google). Hence, this plays a major role in systems migrating to or behind hypergiants, besides all the existing economic incentives of centralization.

However, these DoS attacks are *enabled* by careless system administration, like operators that leave amplifiers readily connected to the Internet or vendors that roll out carelessly-thrown together IoT devices, shipped with default credentials. It has become the custom to provide services and run infrastructure without taking responsibility and caring for its impact on others.

Proposition 3

> *There is a tension between privacy and security pitting decentralization vs. centralization.*

A major component of centralization and migrating to centralized cloud infrastructures is the reduction of capital expenses in terms of knowledge. While this means that organizations become dependent as they no longer retain the ability to run their own infrastructure [10], it also hints at the issue of security being 'easier' for centralized clouds.

While security in itself is already easier in a centralized 'walled garden'—simply because there is more knowledge on what is *normal* to work with and detect anomalies—it is also easier when there are the resources there to run systems *properly*. A dedicated security

team is simply unrealistic for smaller organizations, let alone small communities. In addition, building a system that tolerates human error [17] and lessens the impact of security misconfigurations [5] needs a certain scale.

Polemically speaking, this ultimately creates a choice between the devil and the deep blue sea: Either you allow a selected hypergiant to—technically be able to—read your emails and their 'walled garden' will keep your mails and you secure. Or you host your own system and might be less able to deliver your mails to others [13], or may even find them leaked due to a configuration mistake.

Proposition 4

Centralization and profit are inherently incompatible with care for infrastructures.

Controlling the infrastructure means power [15, 31]. In our global economy, this power is accumulated by corporations, which naturally have the goal of maximizing their profit.

This aspect is, in our perspective, inherently incompatible with care for systems as specified in Proposition 1. Caring for systems and users' needs is costly. Needs are always diverse, and applying appropriate care lets you digress from the cattle-style approach needed in scaling operations [19].

Hence, in a profit-oriented world, it can become fiscally untenable to maintain sufficient care for a service and its users. To conserve their bottom line, corporations will discontinue services users rely on, or apply support mechanics that can not provide the care some users may need. While for a corporation, this is a rational decision, it will mean a significant loss for users, no matter how mundane (your fancy home automation no longer working [1]), unusual, or obviously essential (visual implants becoming obsolete [34]) a service is.

Proposition 5

We have to be prepared for hypergiants' failing.

As unusual as the idea of Amazon, Facebook, Apple, and Google going bankrupt or disappearing may sound, it is a possibility we must expect. Similar to Lehman Brothers having been considered too big to fail, we do not expect these hypergiants to disappear either.

Small ripples can cause a hypergiant to tumble, and our burning world is sending out the first signals. Infrastructure supported by the exploitation of labor in a globalized world will not sustain itself forever [23]. Moreover, the skyrocketing energy prices cause issues for major energy consumers, and a single data center can consume the equivalent electricity of 50,000 homes [33].

Ultimately, for the Internet, though, the question of *why* hypergiants fail is not essential. The important question is how we handle them disappearing when the majority of websites contains fonts hosted by, e.g., Google [7, 22], while dealing with legacy systems remains a major issue [25].

Proposition 6

Communities caring for local and distributed infrastructure are the future in a world falling apart.

Our world is changing and—by our own hands—not necessarily for the better. So, following the question of what we do when the hypergiants fail, we also have to ask ourselves what we could do when even more significant parts of the Internet fail in the shifts to come.

Rapenne, an OpenBSD developer, published a thought experiment on rebuilding the world based on the central assumption that *"[...] we would still have *some* power available [...]"* [30]. Her worth reading future scenario involves having generators and solar panels while the surroundings are littered with computers and network technology. As those could be used to run local (potentially interconnected) networks (of networks), this could provide primary services for communities.

This perspective on critical IT infrastructure contradicts the further evolution of the platform economy and centralization of the current Internet. We project that the task of 'making it run even though the cloud controller is gone' will be an essential occupation in a potential future. Local communities will (have to) find ways to utilize technology and provide working services.

Proposition 7

The slow adoption of IPv6 hinders a re-decentralization of the Internet.

The IPv4 address space is, for all practical matters exhausted and in any case globally unjustly distributed [26]. With the Internet still being very much IPv4 centric—at least when it comes to the path *outside* of hypergiants—communities running their own services still *need* IPv4 addresses to provide services. Considering the state of the IPv4 address market, this would mean an investment of tens of thousands of dollars [1]. While this is a prohibitive cost for a small community project, it enables hypergiants and large hosting corporations to further collect addresses on a relatively cheap price compared to their annual operating expenses, thereby further centralizing the Internet [12, 20, 21]. If we want to re-distribute the Internet, the IPv6 migration is imperative.

Proposition 8

In a burning world, functionality is more important than security, but remains trumped by safety.

If we ever—and we hope it does not come to it—face a world burnt to its foundations, with an Internet fallen apart and hypergiants failed, paradigms of 'what is important' will shift dramatically. We will find ourselves in a situation where the utility and functionality of systems will superimpose their security even stronger as in the current world. We predict that in such a world, threat modeling will see a significant shift away from security against threats from the larger Internet, back towards the question of *'What harm can be done if it is not secure?'*. Essentially, threat modeling will become a question of *safety* [9]. Ultimately, the physical safety of local communities will have the highest importance.

[1] At the time of writing the IPv4 address price hovered around $60 per address.

Proposition 9

Systems that are too complex to be understood by a single person cannot be sustainable.

Over the past decades, IT systems have become increasingly complex. There are countless discussions about the explosion in complexity of protocols, for example email [13], and the 'DNS Camel' [3] is certainly one of the most iconic illustrations of this issue. Furthermore, this trend continues into the operation of systems. While the introduction of Infrastructure-as-Code, and DevOps aims to make systems more maintainable and succeeds in certain contexts, it also adds layer upon layer of abstraction. To illustrate this issue with an anecdote: When we tried to set up monitoring for a small self-hosted video conferencing setup supporting a faculty in teaching during the COVID-19 pandemic, we ultimately ended up using decades-old monitoring software. We did so because all more recent monitoring tools would drag along a software stack as complex, and sometimes even more complex, than the setup it was supposed to monitor.

Again, Rapenne provided the foundation of this proposition in a blog article [29]. This article succeeds in dissecting the reliance of automation and complex systems on its building blocks that need to be understood before they can be 'abstracted away'. However, to be sustainable in a burning world, systems will have to be run (and understood) by small teams and communities (see Proposition 7). Hence, while in an ever-growing and centralizing Internet automation is a necessity, its complexity might become a curse in an Internet that is supposed to survive in a burning world. Or, to put it in an example: Without a central docker repository, there is no place where `curl | sudo bash` can pull the image from.

Proposition 10

Systems should enable a better tomorrow and not burn the world even further.

The aforementioned increasing complexity of systems also adds back to their resource hunger. However, with the wide availability of automation and support infrastructure—which of course has their good in *enabling* many people to build—these systems are being used, adding to a growing ball of systems supporting other systems in abstracting something simple to something more complex. This, in turn, eats itself into how we build and design systems, adding layers and utilizing more resources for the *same* functionality. This development has been brought to the extreme by Bitcoin and its proof-of-work siblings, churning through energy on a nation-state scale [14], while having no *purpose* except for profit. Bitcoin may very well be the perfect piece of performance art, illustrating the fall of a species burning its planet in the strife for *more*, merely for the sake of *more*.

As such, we claim that it is an engineer's responsibility to ensure that the systems they build contribute to a beneficial purpose and do not harm society or the environment by needless and redundant processing.

Proposition 11

There are no technical solutions for social and societal problems.

This proposition is a long-standing dictum in the German hacker community. It originates around the observation that local communities of hackers will often try to fiddle together a technical solution if they encounter a social problem. The most commonly experienced situation is the issue of 'unreliable' payments being provided for the drinks usually available via a public fridge, paid for in an honor system. Usually and periodically, several tech-savvy people start to implement a complex digital cash-and-credit system to solve this issue, usually in a way that also includes a touch-screen and a RasberryPi. Ultimately, that approach will suffer from limited adoption and the same issues as before, and a social solution will have to be found. If the community is *very* unlucky, the technical solution also introduces *new* social problems. The insufficient solution nevertheless stays in place, usually until the next generation of local nerds experiences this issue, and repeats the circle. To summarize this with colloquial wisdom from the "Industry 4.0" and production industry: "Digitizing a shitty process won't result in a better process, but in a digitized shitty process".

The point here is that we try to apply the same reasoning to problems we are facing at the much larger scale of the Internet. The problem is that this solution mechanism outlined above is also used at the much larger scale of the Internet. We consistently face the impact of—ultimately—social and societal issues (operators announcing routes they should not [4], attackers launching DoS attacks using amplifiers—and operators running amplifiers or failing to implement BCP38 [2, 8, 18]). To counter them, we developed technical solutions, for example, RPKI to handle the issue of routes being announced by entities that should not announce them. Given the example of the drink accounting system, though, the real question is, what a better solution would be.

Proposition 12

Internet sanctions: What once has been thought can never be taken back. The Internet will be falling apart.

This proposition starts with a quote from Friedrich Dürrenmatt's *"Die Physiker"* and ties tightly with Proposition 10. In his book, this quote relates to a physicist's perspective on the probability of keeping one's dangerous inventions—ultimately an analogy for nuclear fission—from the world. However, it is also highly relevant in terms of the Internet as technology and proposals *with certainly good intentions* are developed. A concrete example: In the wake of the war waged by Russia against Ukraine, members of the Internet community and several politicians called for a multi-stakeholder approach to 'Internet Sanctions' [35]. In short, the authors of that open letter call for a multistakeholder mechanism that populates databases, which willing Internet participants can utilize to participate in sanctions against specific netblocks and domains, ideally by using existing infrastructure for blocklisting IP routes.

However, this means that due to the tiered nature of the Internet the optionality of this approach is severely limited for network participants relying on upstream providers, as long as enough

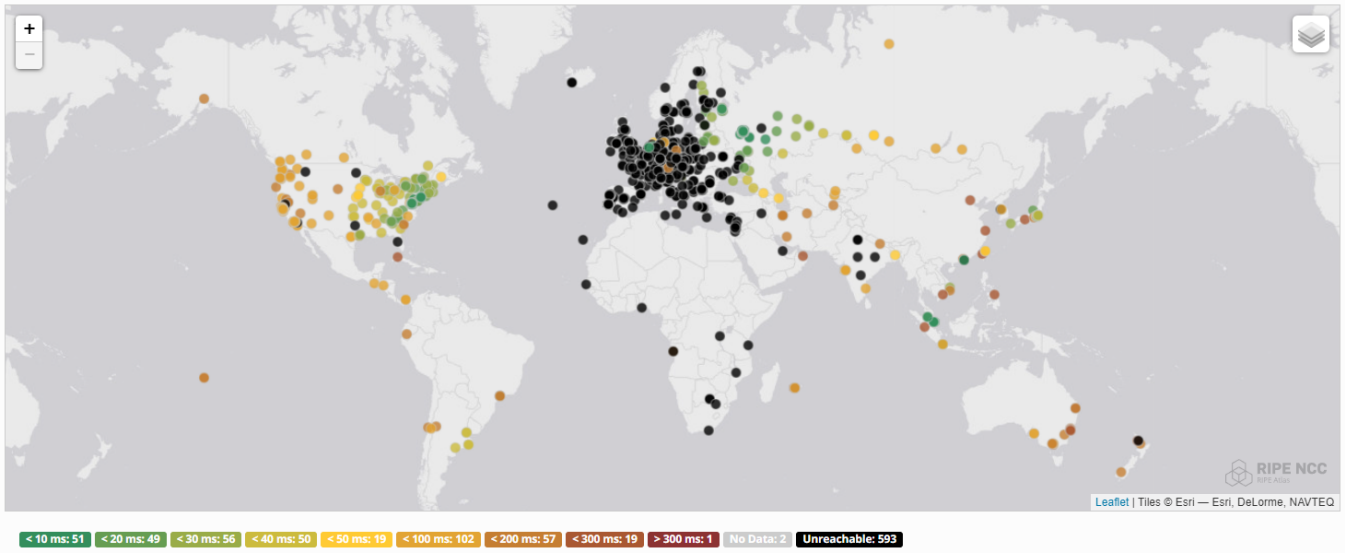

Figure 1: Reachability of `178.248.233.26` (Sputnik News) in RIPE Atlas after Internet sanctions were applied [27].

Tier 1/Tier 2 operators participate. For reference, see Figure 1, which depicts the reachability of `178.248.233.26` (Sputnik News) from RIPE Atlas probes after sanctions were applied. We see that the address is unreachable from Europe, but also from the AFRINIC region which regularly transits through Europe. Yet, other global north regions, e.g., the U.S. and Australia, show a significantly higher reachability.

Furthermore, and this is the far more crucial point, this case demonstrates that it *is* possible to sanction specific IP addresses and networks. In the past approaches against, e.g., `piratebay.org` or `wikileaks.org` were mostly circumventable DNS based blocking attempts [24], with the organized chiming of the Internet community that blocking individual sites is not really possible unless a system like a 'Great National Firewall' is implemented. The Internet now success demonstrated that state sanction blocking of resources *is* possible. We claim that policy makers will not forget this, and this approach will find its use in the future again. It will also put Internet sanctions on the diplomatic agenda, and in turn lead to a fragmentation of the Internet.

Proposition 13

Digital sovereignty is being used wrong.

Digital sovereignty is currently one of the most pressing issues in the digital policy arena [32]. However, it is usually understood as *'ensuring that a state can exert policy on the systems used by its constituents, while ensuring that only their own policy is applied to them.'* The classical example of attempts to realize this with policy is most likely the ongoing discussion of the 'Safe Harbor'. The more technical approach is 'Schengen Routing' [6].

However, in either case, the more fundamental meaning of sovereignty is usually missed: The ability to (re)build and maintain one's infrastructure independent of another party.

One might argue that this is not an issue in a globalized world. Yet, in a burning world, it may be essential to have the know how to keep systems running wide spread and locally available. Coming back to the sum of the earlier propositions, the policy aspect may even be secondary. In the end it is about running systems, providing services, and caring for users. Everywhere. As long as we can rebuild.

2 CONCLUSION

This paper presents thirteen propositions around a resilient and sustainable Internet, which should be run with care for its users and the infrastructure itself. They might be overly bold, lack concrete solutions, and paint a disturbingly dire picture of the world.

Still, given the state of the world, we claim that we are past the point of raising awareness and hiding behind 'they would never'; We can no longer risk staying complacent in the hopes for a better future. We have to talk about these issues *now* and find tangible solutions. The future will be bleak if we do not make it better, and whether the world goes down in flames or not, preparation is better than reaction.

ACKNOWLEDGEMENTS

This material is based upon work partially supported by the European Commission through the H2020 project CyberSecurity4Europe (Grant No. #830929). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of their host institutions or those of the European Commission.

REFERENCES

[1] Ara Wagoner. 2020. *Nest Secure is being discontinued and current owners are losing their minds.* https://www.androidcentral.com/nest-secure-being-discontinued-and-people-are-rightfully-losing-their-minds

[2] F. Baker and P. Savola. 2004. Ingress Filtering for Multihomed Networks. RFC 3704 (Best Current Practice). https://doi.org/10.17487/RFC3704 Updated by RFC 8704.

[3] Bert Hubert. 2018. *Herding the DNS Camel.* https://www.ietf.org/blog/herding-dns-camel/

[4] Shinyoung Cho, Romain Fontugne, Kenjiro Cho, Alberto Dainotti, and Phillipa Gill. 2019. BGP hijacking classification. In *2019 Network Traffic Measurement and Analysis Conference (TMA)*. IEEE, 25–32.

[5] Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. 2018. Investigating system operators' perspective on security misconfigurations. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 1272–1289.

[6] Daniel Dönni, Guilherme Sperb Machado, Christos Tsiaras, and Burkhard Stiller. 2015. Schengen routing: a compliance analysis. In *IFIP International Conference on Autonomous Infrastructure, Management and Security*. Springer, 100–112.

[7] Steven Englehardt and Arvind Narayanan. 2016. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 1388–1401.

[8] P. Ferguson and D. Senie. 2000. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. RFC 2827 (Best Current Practice). https://doi.org/10.17487/RFC2827 Updated by RFC 3704.

[9] Tobias Fiebig. 2020. How to stop crashing more than twice: A Clean-Slate Governance Approach to IT Security. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 67–74.

[10] Tobias Fiebig, Seda Gürses, Carlos H Gañán, Erna Kotkamp, Fernando Kuipers, Martina Lindorfer, Menghua Prisse, and Taritha Sari. 2021. Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds. *arXiv preprint arXiv:2104.09462* (2021).

[11] Tobias Fiebig, Franziska Lichtblau, Florian Streibelt, Thorben Krüger, Pieter Lexis, Randy Bush, and Anja Feldmann. 2018. Learning from the past: designing secure network protocols. In *Cybersecurity Best Practices*. Springer, 585–613.

[12] Vasileios Giotsas, Ioana Livadariu, and Petros Gigis. 2020. A first look at the misuse and abuse of the IPv4 Transfer Market. In *Proceedings of the Passive and Active Measurement Conference*. Springer, 88–103.

[13] Florian Holzbauer, Johanna Ullrich, Martina Lindorfer, and Tobias Fiebig. 2022. Not that Simple: Email Delivery in the 21st Century. In *USENIX Annual Technical Conference (ATC)*.

[14] Shangrong Jiang, Yuze Li, Quanying Lu, Yongmiao Hong, Dabo Guan, Yu Xiong, and Shouyang Wang. 2021. Policy assessments for the carbon emission flows and sustainability of Bitcoin blockchain operation in China. *Nature communications* 12, 1 (2021), 1–10.

[15] Dal Jong Jin. 2015. *Digital Platforms, Imperialism and Political Culture.* Routledge.

[16] Mannat Kaur, Simon Parkin, Marijn Janssen, and Tobias Fiebig. 2022. "I needed to solve their overwhelmness": How system administration work was affected by COVID-19. *ACM Computer Supported Cooperative Work (CSCW)* (2022).

[17] Mannat Kaur, Michel van Eeten, Marijn Janssen, Kevin Borgolte, and Tobias Fiebig. 2021. Human Factors in Security Research: Lessons Learned from 2008-2018. *arXiv preprint arXiv:2103.13287* (2021).

[18] Franziska Lichtblau, Florian Streibelt, Thorben Krüger, Philipp Richter, and Anja Feldmann. 2017. Detection, classification, and analysis of inter-domain traffic with spoofed source IP addresses. In *Proceedings of the ACM Internet Measurement Conference*. 86–99.

[19] Thomas A Limoncelli, Christina J Hogan, and Strata R Chalup. 2016. *The Practice of System and Network Administration: Volume 1: DevOps and other Best Practices for Enterprise IT*. Vol. 1. Addison-Wesley Professional.

[20] Ioana Livadariu, Ahmed Elmokashfi, and Amogh Dhamdhere. 2017. On IPv4 transfer markets: Analyzing reported transfers and inferring transfers in the wild. *Computer Communications* 111 (2017), 105–119.

[21] Ioana Livadariu, Ahmed Elmokashfi, Amogh Dhamdhere, and KC Claffy. 2013. A first look at IPv4 transfer markets. In *Proceedings of the ACM Conference on Emerging Networking Experiments and Technologies*. 7–12.

[22] Stephen Ludin. 2017. Measuring what is not ours: A tale of 3rd party performance. In *Proceedings of the Passive and Active Measurement Conference*, Vol. 10176. Springer, 142.

[23] Natalie Sherman. 2022. *Amazon workers win battle to form first US union.* https://www.bbc.com/news/business-60944677

[24] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. 2017. Global measurement of DNS manipulation. In *26th USENIX Security Symposium (USENIX Security 17)*. 307–323.

[25] Stijn Pletinckx, Kevin Borgolte, and Tobias Fiebig. 2021. Out of Sight, Out of Mind: Detecting Orphaned Web Pages at Internet-Scale. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 21–35.

[26] Philipp Richter, Mark Allman, Randy Bush, and Vern Paxson. 2015. A primer on IPv4 scarcity. *ACM SIGCOMM Computer Communication Review* 45, 2 (2015), 21–31.

[27] RIPE Atlas. 2022. *one-off IPv4 Ping "Ping measurement to 178.248.233.26" id 40859682.* https://atlas.ripe.net/measurements/40859682/#map

[28] Christian Rossow. 2014. Amplification Hell: Revisiting Network Protocols for DDoS Abuse. In *Proceedings of the ISOC Network and Distributed Systems Security Symposium*.

[29] Solène Rapenne. 2021. *Obsolete in the IT crossfire.* https://dataswamp.org/~solene/2021-07-09-obsolete-feeling-in-the-crossfire.html

[30] Solène Rapenne. 2021. *What if Internet stops? How to rebuild an offline federated infrastructure using OpenBSD.* https://dataswamp.org/~solene/2021-10-21-huge-disaster-recovery-plan.html

[31] Nick Srnicek. 2017. *Platform Capitalism.* Wiley & Sons.

[32] Pierantonia Sterlini, Fabio Massacci, Natalia Kadenko, Tobias Fiebig, and Michel van Eeten. 2019. Governance Challenges for European Cybersecurity Policies: Stakeholder Views. *IEEE Security & Privacy* 18, 1 (2019), 46–54.

[33] Steven Gonzalez Monserrate. 2022. *The Staggering Ecological Impacts of Computation and the Cloud.* https://thereader.mitpress.mit.edu/the-staggering-ecological-impacts-of-computation-and-the-cloud/

[34] Eliza Strickland and Mark Harris. 2022. *Their Bionic Eyes are now Obsolete and Unsupported.* https://spectrum.ieee.org/bionic-eye-obsolete

[35] Various Authors. 2022. *Multistakeholder Imposition of Internet Sanctions.* https://www.pch.net/resources/Papers/Multistakeholder-Imposition-of-Internet-Sanctions.pdf