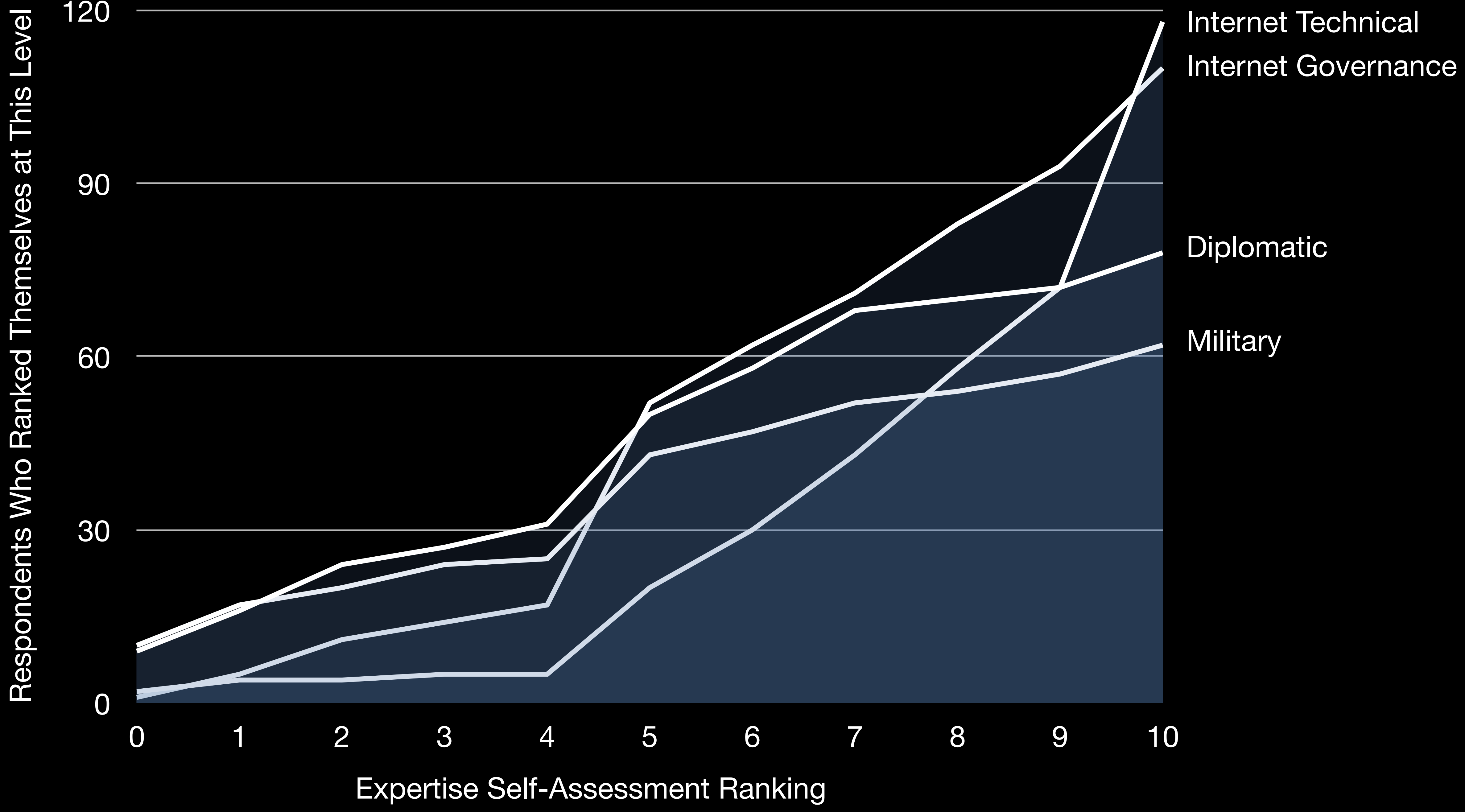
Report of the GCSC Critical Infrastructure Assessment Working Group

November 20-21 2017
Delhi

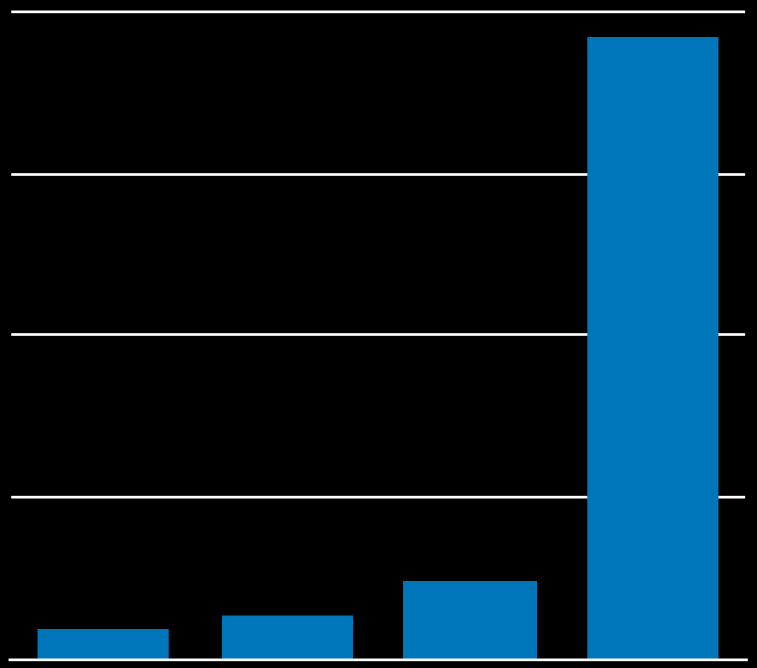
This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Respondent Expertise Self-Assessment

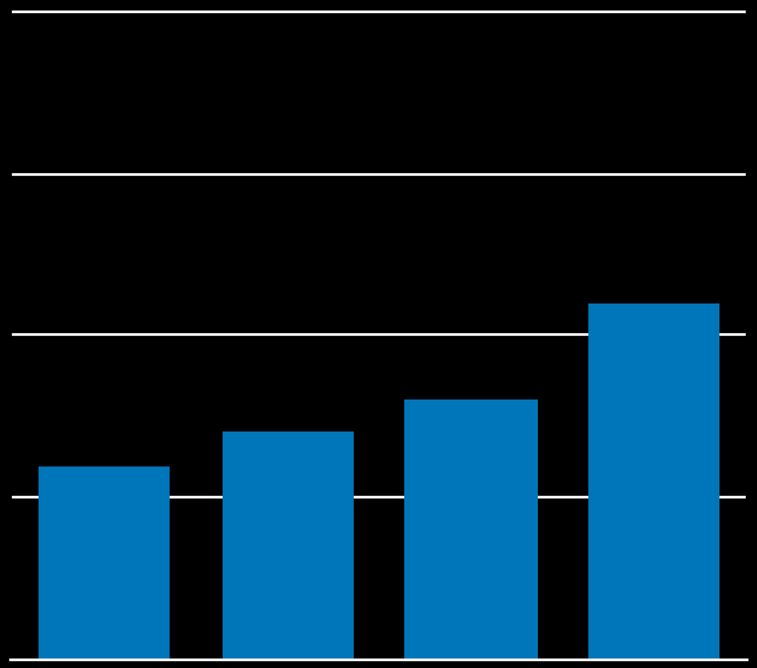


This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Understanding the Graphs



High Degree
of Agreement



Low Degree
of Agreement

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Internet-Accessible and ICT-Enabled Non-Internet Infrastructures

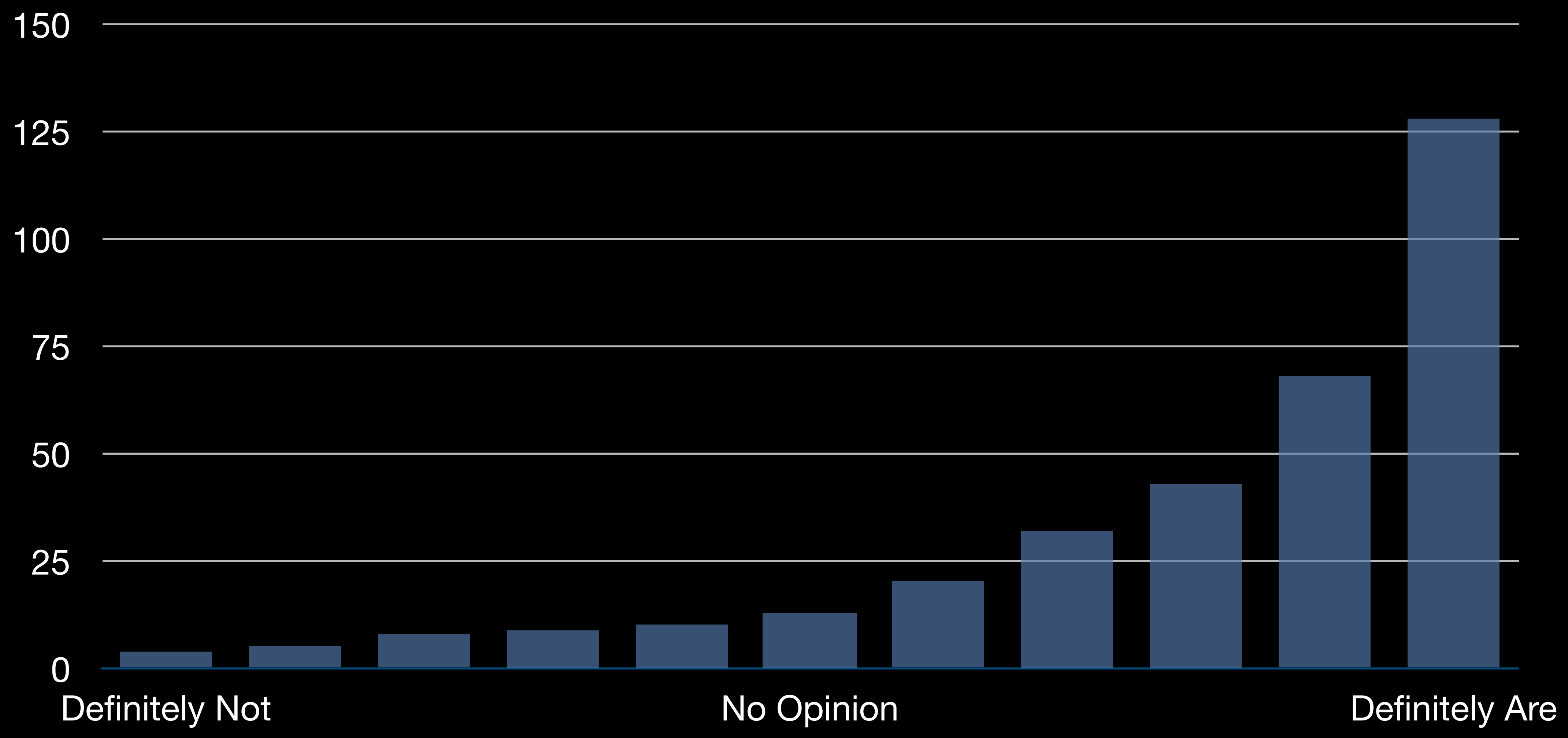
Consider the Internet-accessible and ICT-enabled aspects of these sectors and systems, and tell us whether you think that they are or are not worthy of protection in a cybersecurity norm.

In all cases, we are discussing civilian infrastructure and in some cases dual-use infrastructure, but not military infrastructure. Also, we're discussing specifically the Internet-accessible and ICT-enabled aspects of these systems and sectors, so for example, in "Maritime Transport," we're interested in systems related to scheduling, traffic control, safety, navigation, and auto-pilot; the portions of the system most subject to cyber-attack.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Transportation

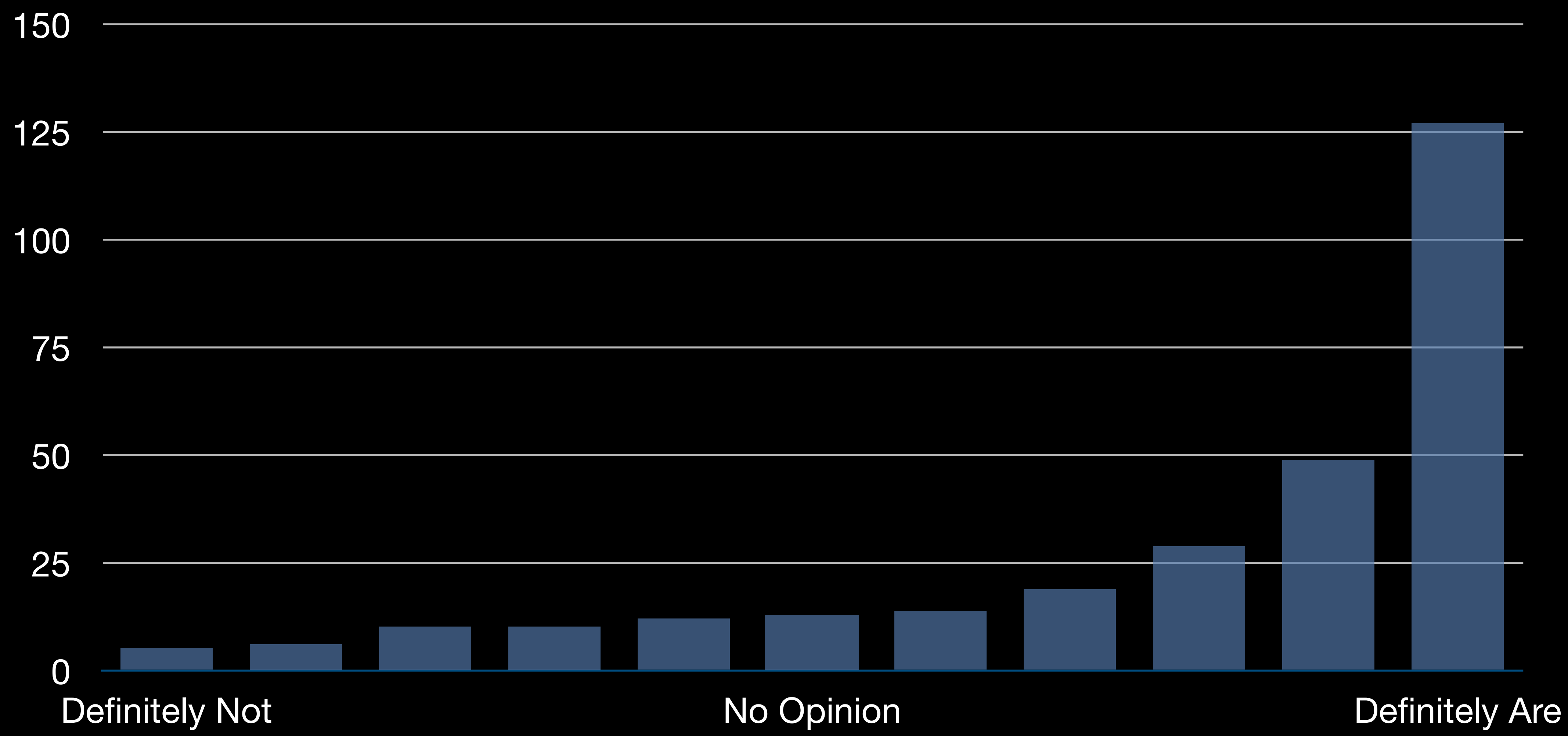
Navigation



Positioning systems for navigation (Gallileo, GPS, BeiDou, Glonass, etc.), including Assisted-GPS terrestrial transmitters and support systems.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

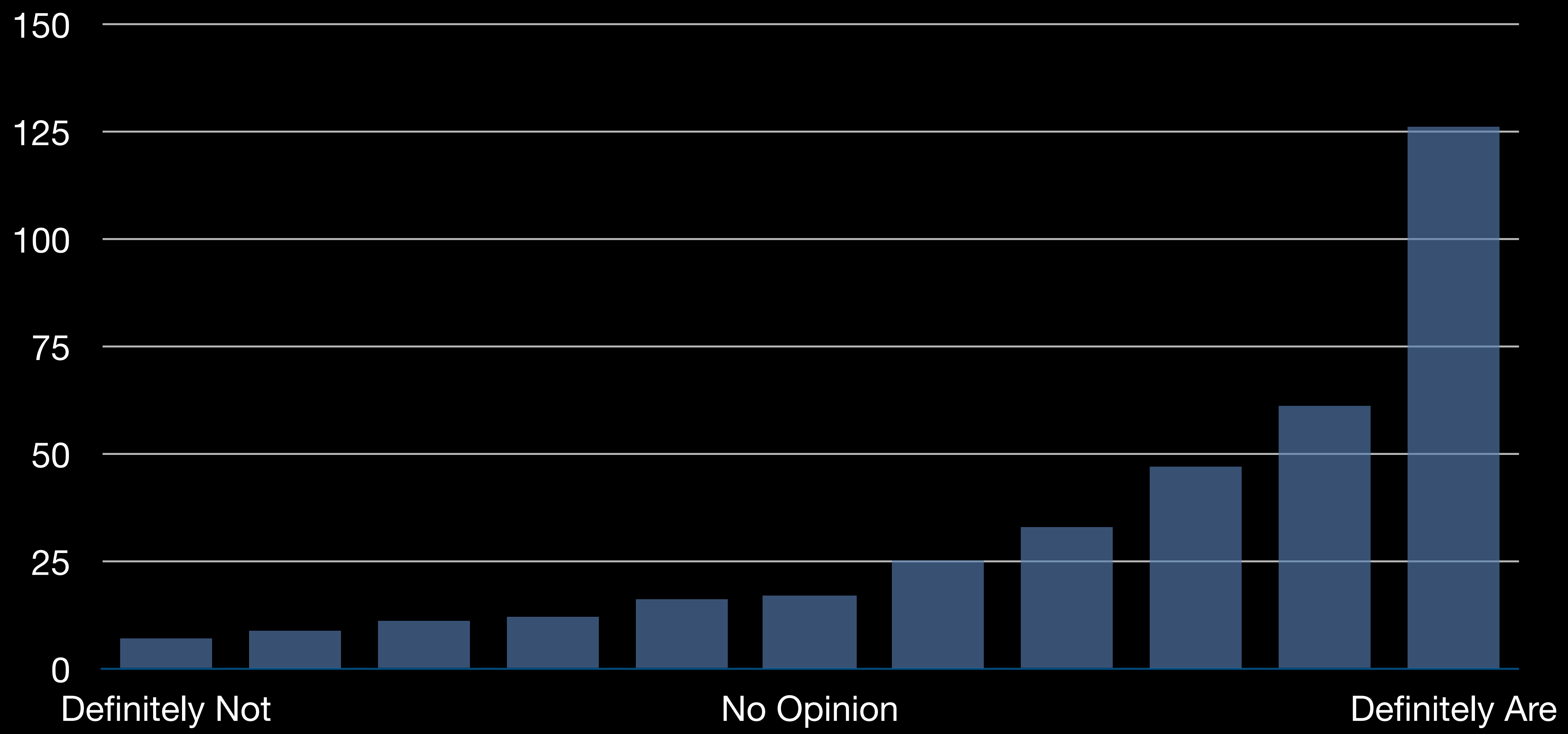
Aviation



Systems for coordinating civil and commercial aviation, including air-traffic control, aircraft-to-ground communications systems, back-end scheduling and resource allocation systems, and ticketing and reservation services.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

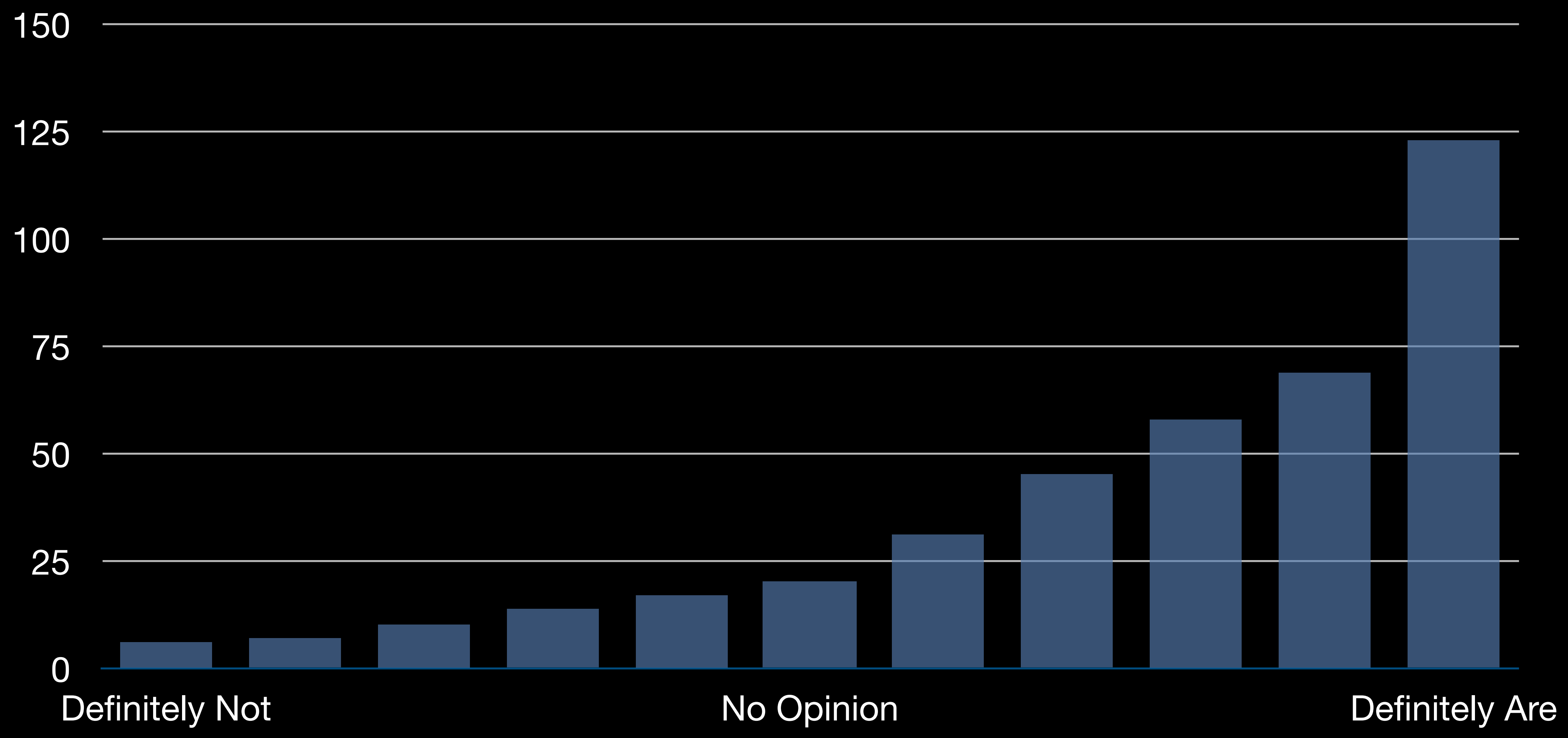
Terrestrial



Systems governing terrestrial transportation and transportation safety. This includes railway safety signaling and control systems, control and safety systems for civilian autonomous vehicles, public transportation and associated ticketing and scheduling systems, and vehicular traffic safety signaling and control systems.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

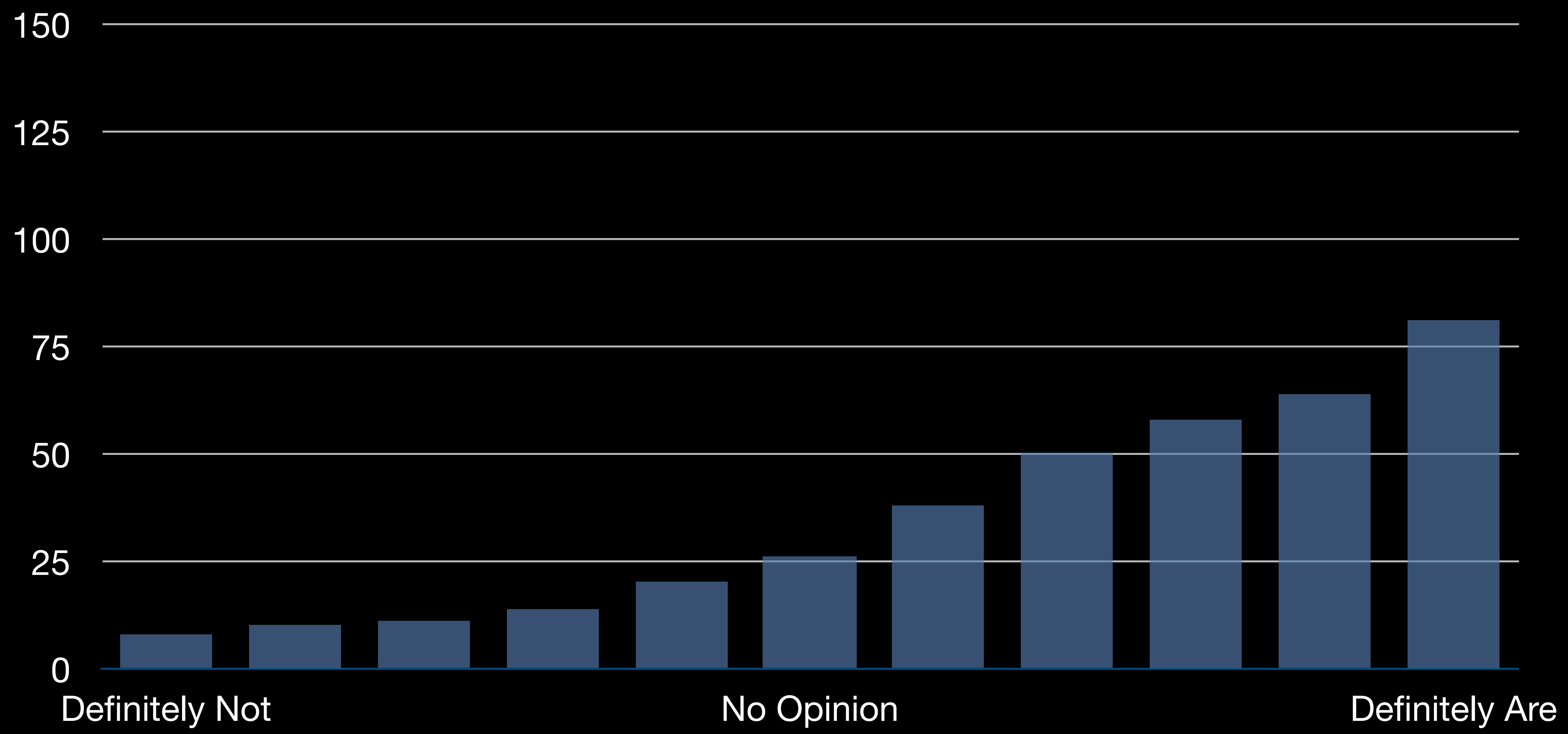
Maritime



Civil maritime passenger and bulk cargo transportation, maritime traffic control systems, and ship-to-shore communications systems.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Intermodal

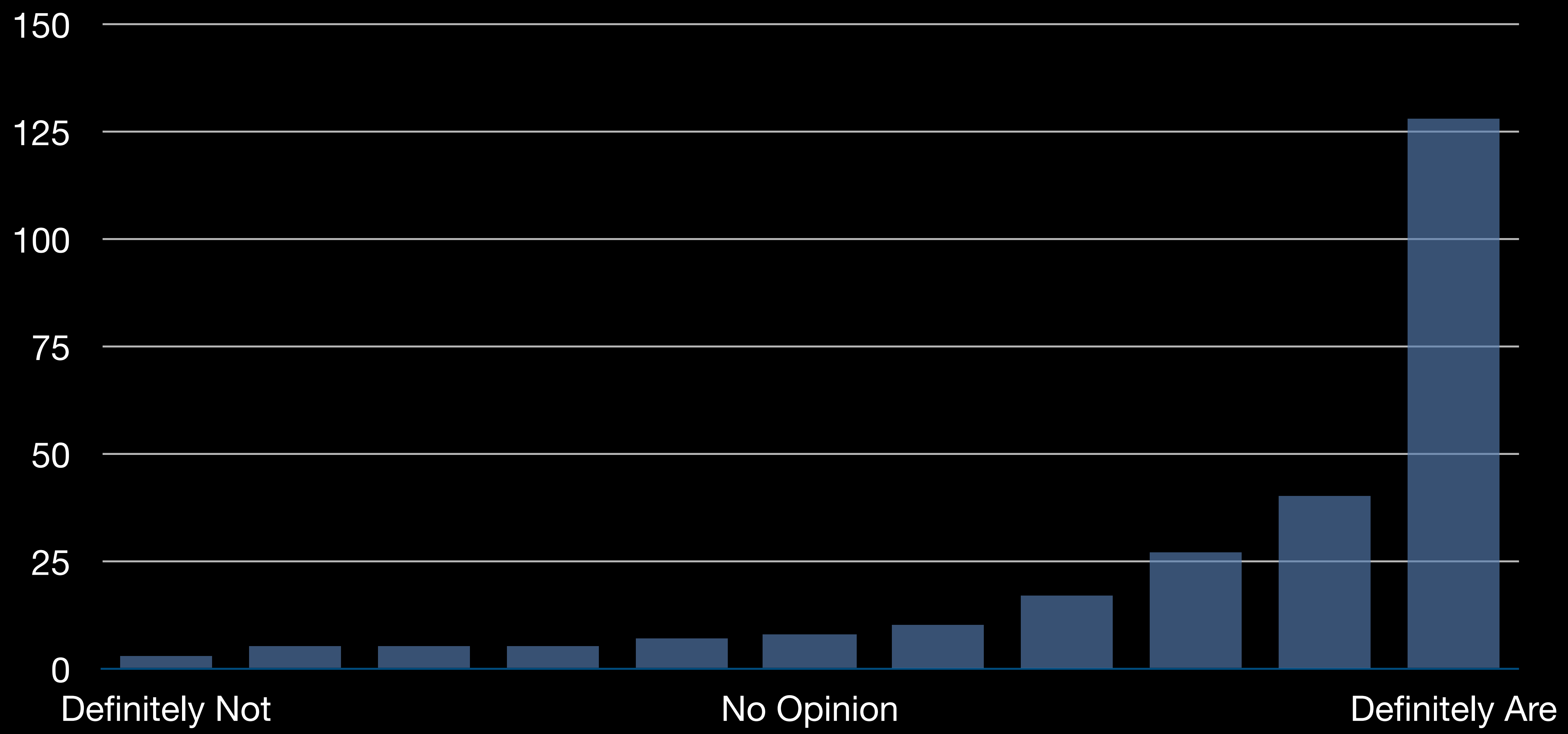


The systems of control and coordination which allow the intermodal transportation of goods via standardized ISO containers by ship, truck, and rail; the door-to-door LTL distribution of the contents of those containers; and the systems which allow for automated bills-of-lading, documentation, and customs-clearing of freight.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Utilities

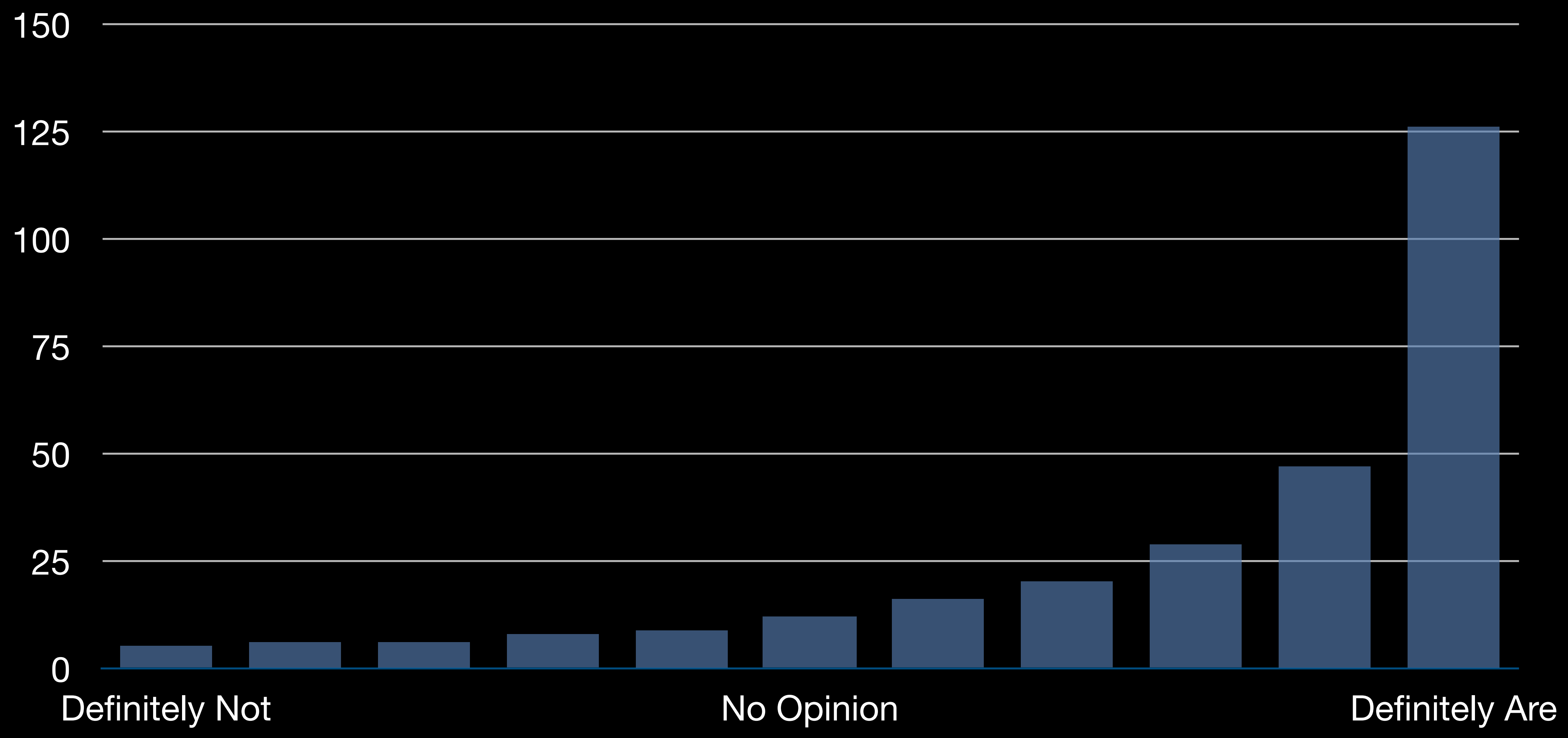
Water



Monitoring and control systems (SCADA, DCS) for controlling and monitoring dams and reservoirs, as well as public water storage, purification, sewage and sewage treatment facilities, flood control, and water distribution systems.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

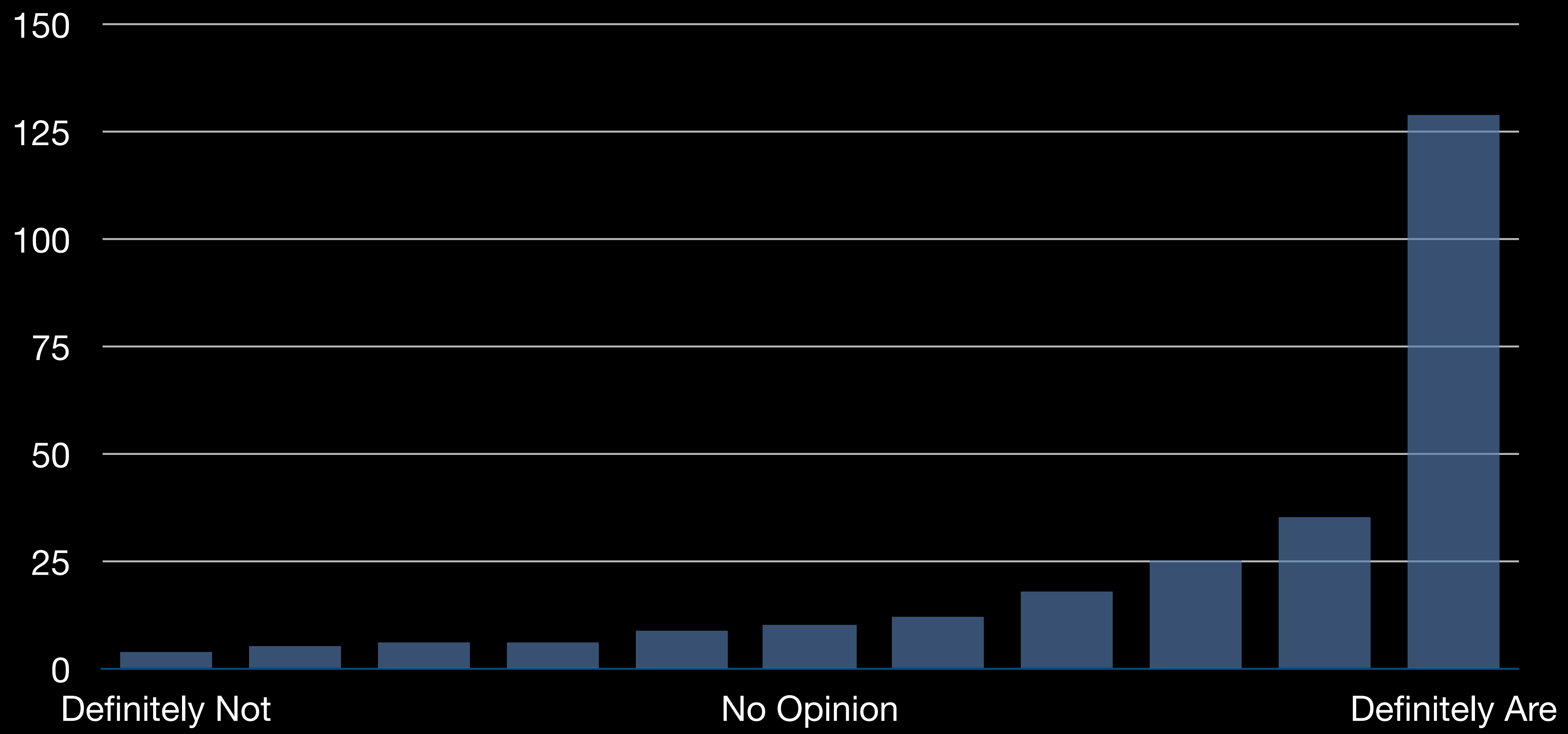
Electricity



Monitoring and control systems for electrical power grid distribution and management, power generation systems, and power utilization meters. (Not including nuclear reactors, which are addressed separately in the next question.)

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

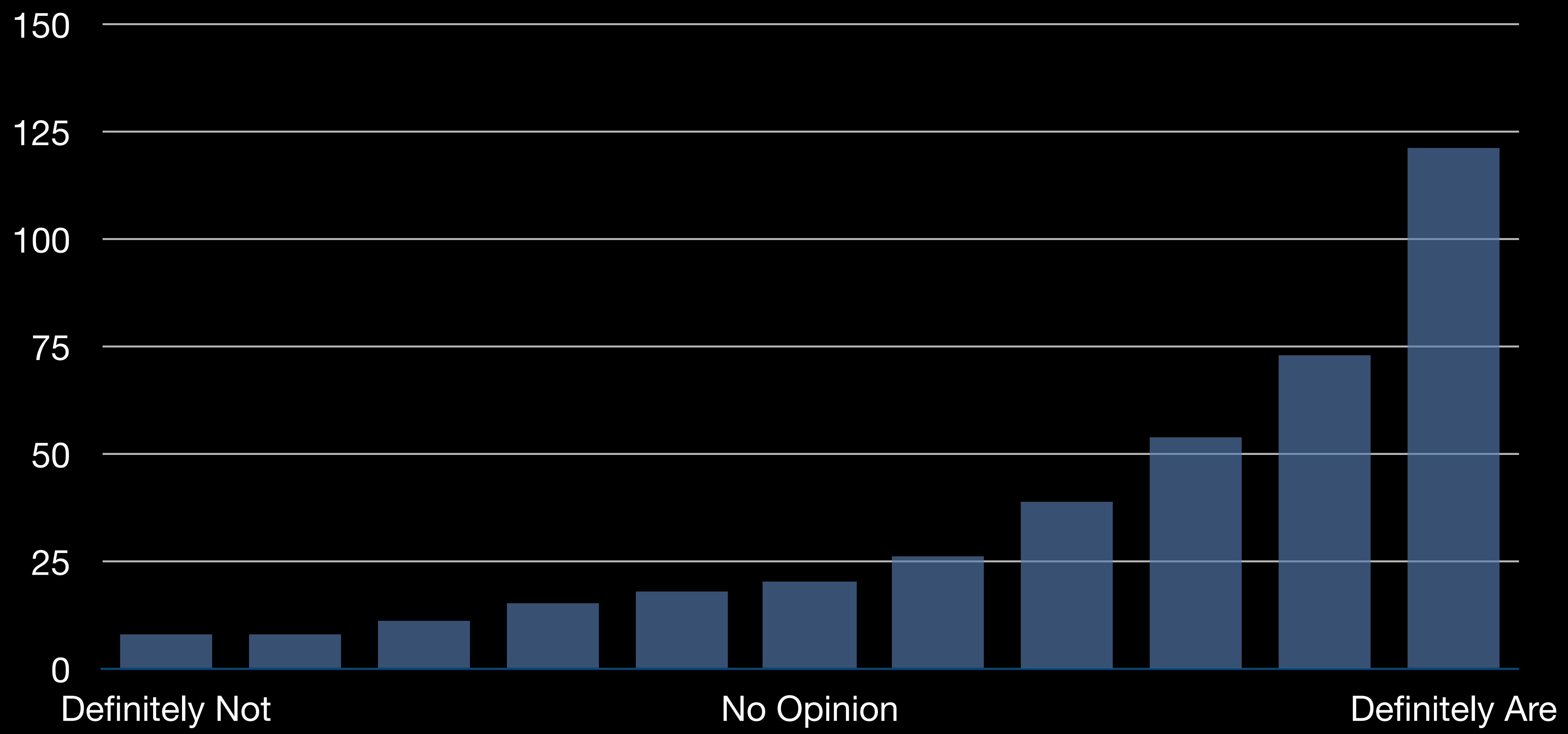
Nuclear



Management systems for nuclear reactors.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Oil & Gas

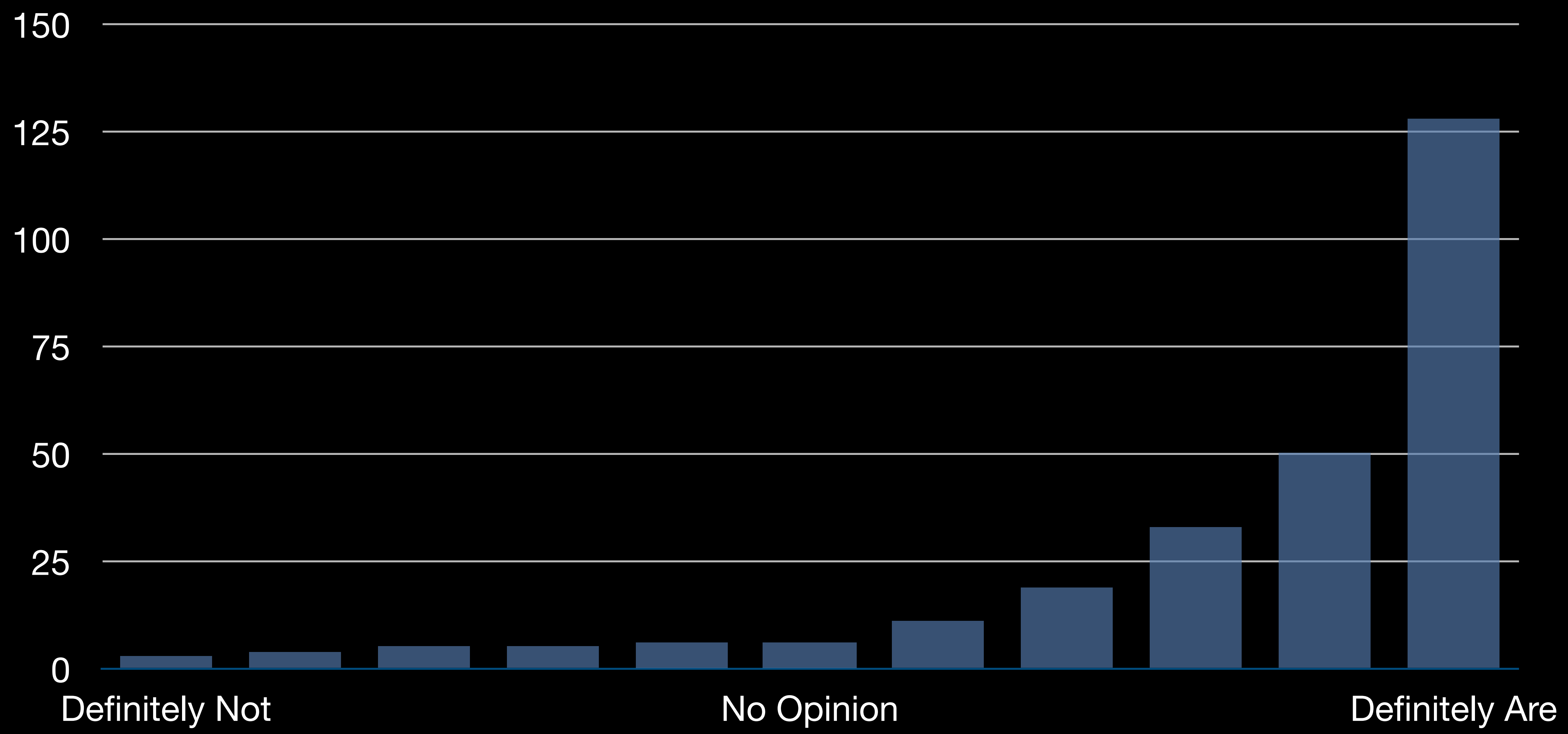


Operational and safety systems for oil and gas pipelines and extraction and refining facilities.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Society

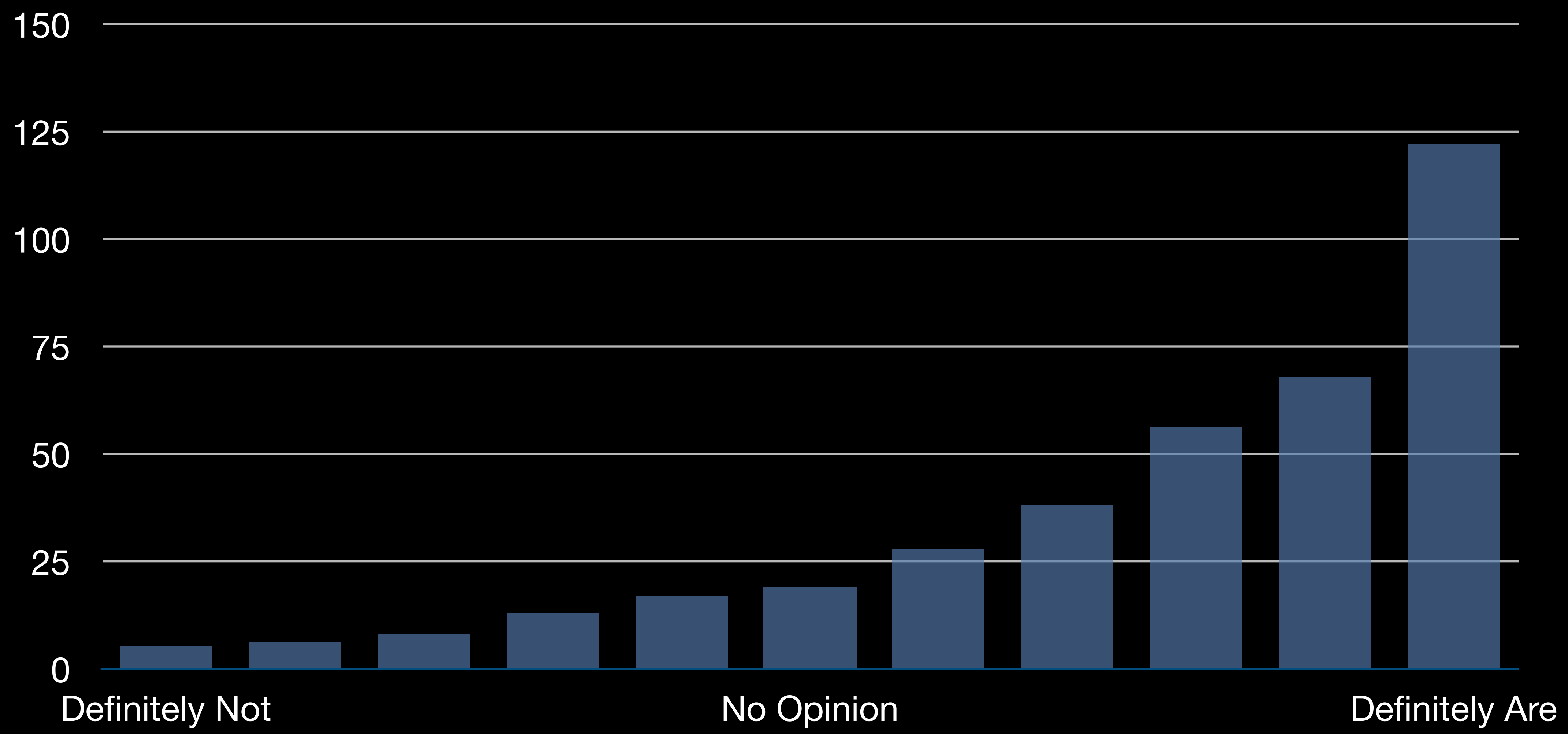
Public Safety



Communications, IT, and monitoring systems related to public safety. This includes systems for emergency communications such as emergency (911/112) call and dispatch centers, hospital and healthcare IT systems, detection and warning systems for natural-disasters (earthquake, fire, hurricane, tsunami, etc.), national computer security incident response organizations (CERTs/CIRTs), and IT systems supporting fire departments, emergency first-responders, and law enforcement.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

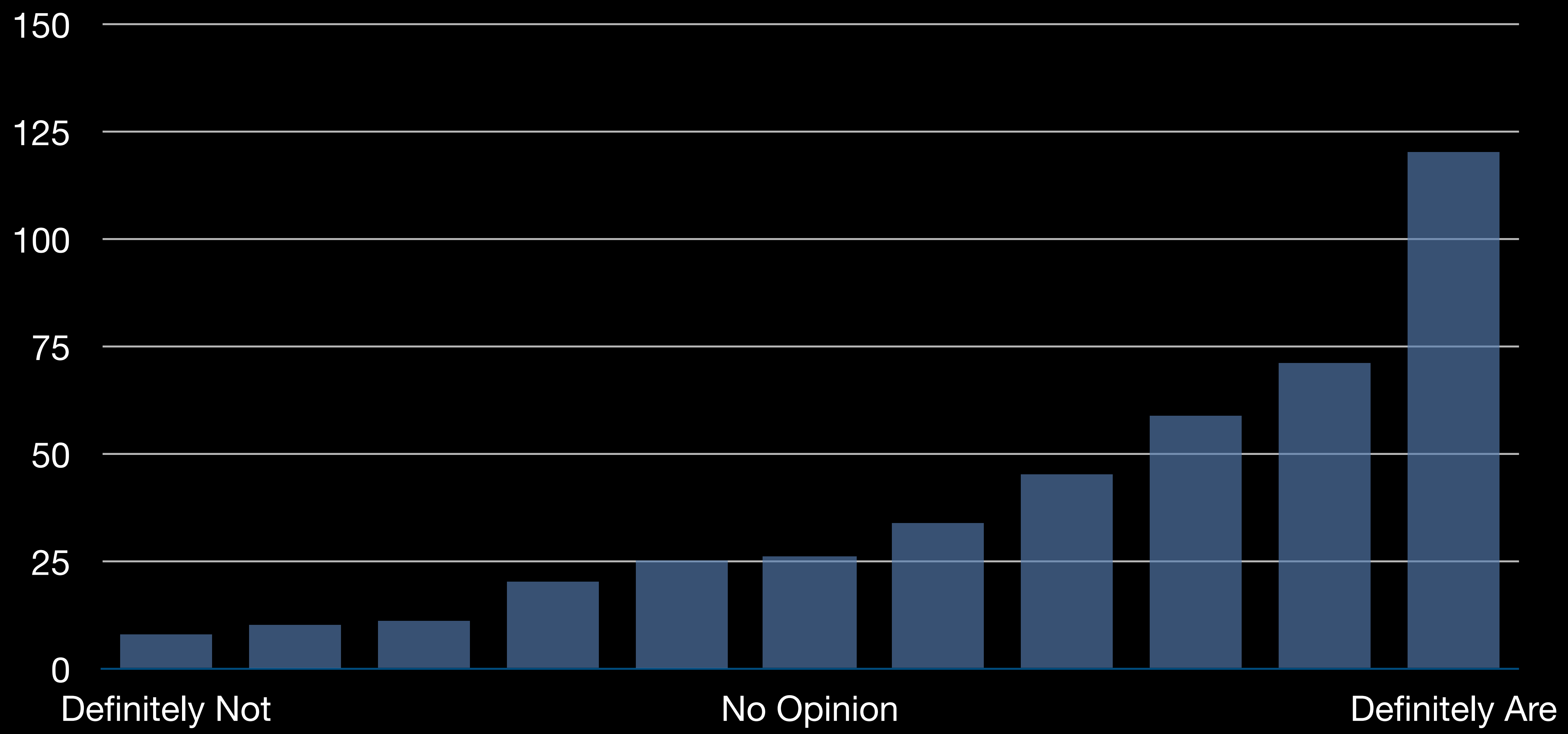
Communications



Systems and infrastructure supporting civilian communications. This includes systems for cellular voice and SMS communication, public radio and television broadcasting, commercial and civilian satellite communications, control and launch systems for commercial and civilian satellites, and postal mail delivery.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

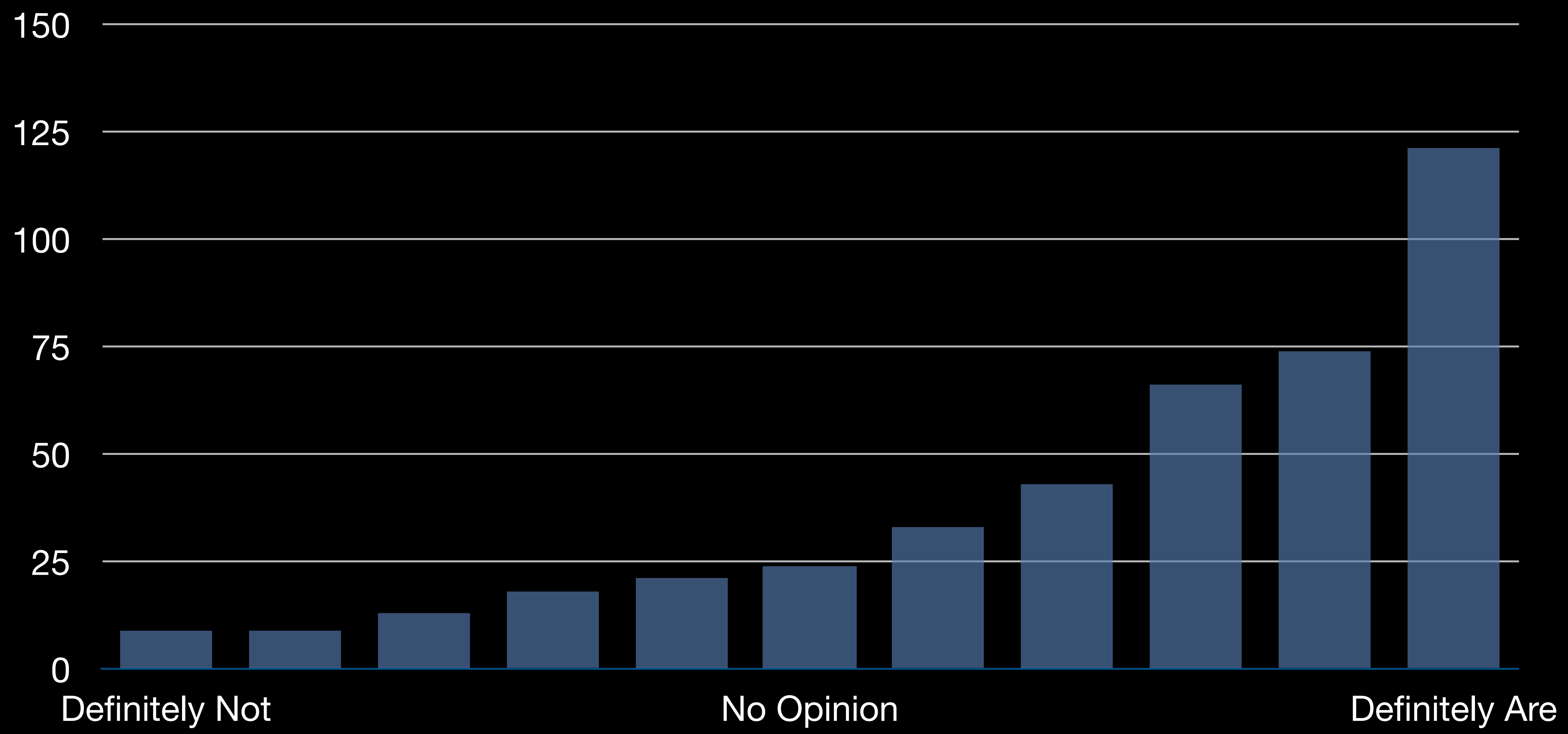
Economy



Systems supporting the functioning of the economy and banking. This includes systems for coordinating financial transactions and transfers (SWIFT, Fedwire, ACH, and interbank/inter-institutional financial settlement systems such as TARGET2, OCC, and DTCC/NSCC), stock and commodity exchanges and associated brokerages for transactions and maintaining records of ownership, the financial services industry and regulated public retail banking and financial services industries, and pension/retirement investment accounts and wealth management services.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

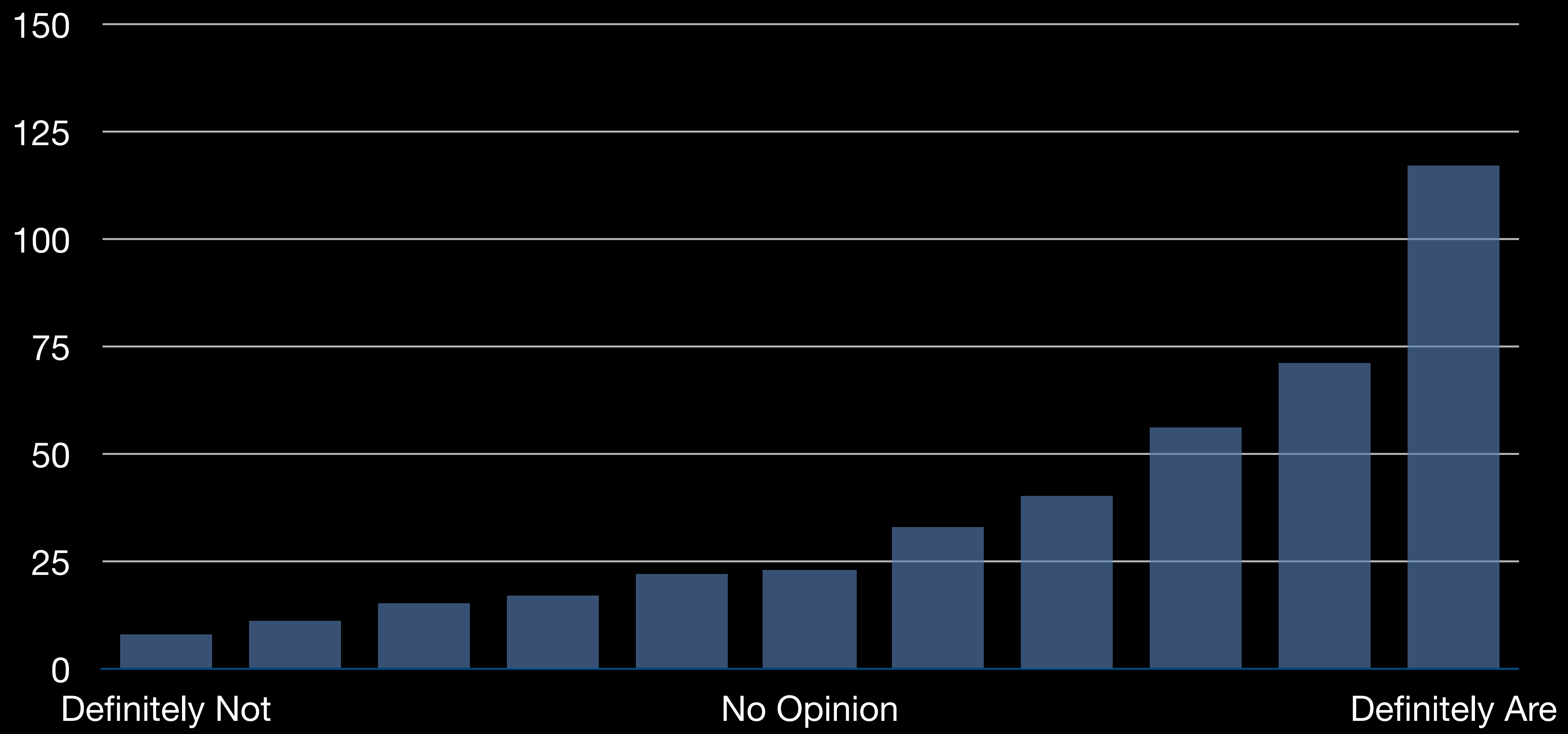
Environment



Monitoring, collection, treatment, and protection systems for managing public and hazardous waste, as well as systems for environmental protection regulation.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

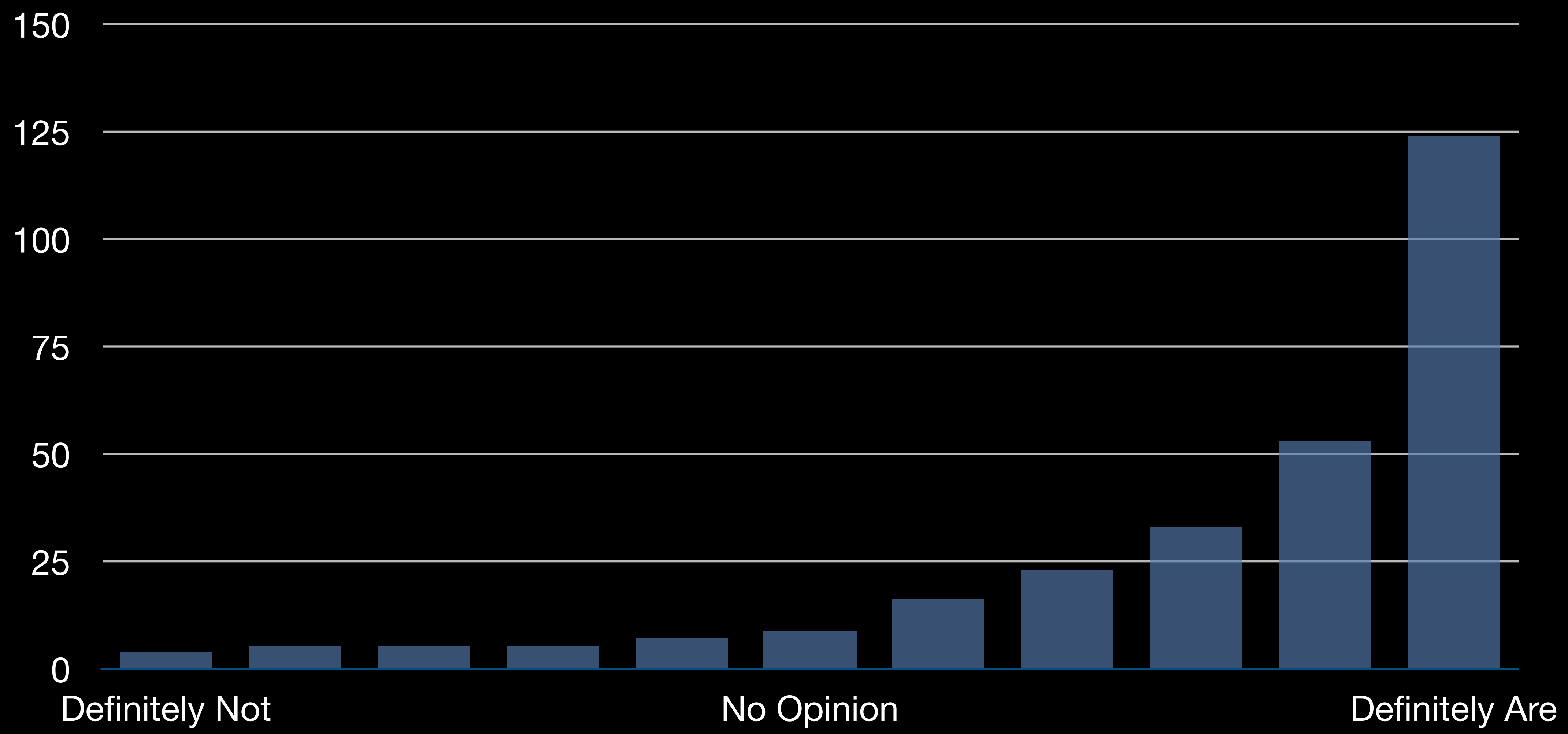
Governance



Systems supporting the functioning of government and democratic institutions. This includes citizenship databases and voter rolls, voting systems, the public and private communications of electoral candidates, international diplomatic communications mechanisms, IT systems supporting the civilian judiciary, and IT systems facilitating governmental services (distributing social services and benefits, taxation, maintaining records of property ownership, etc.).

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

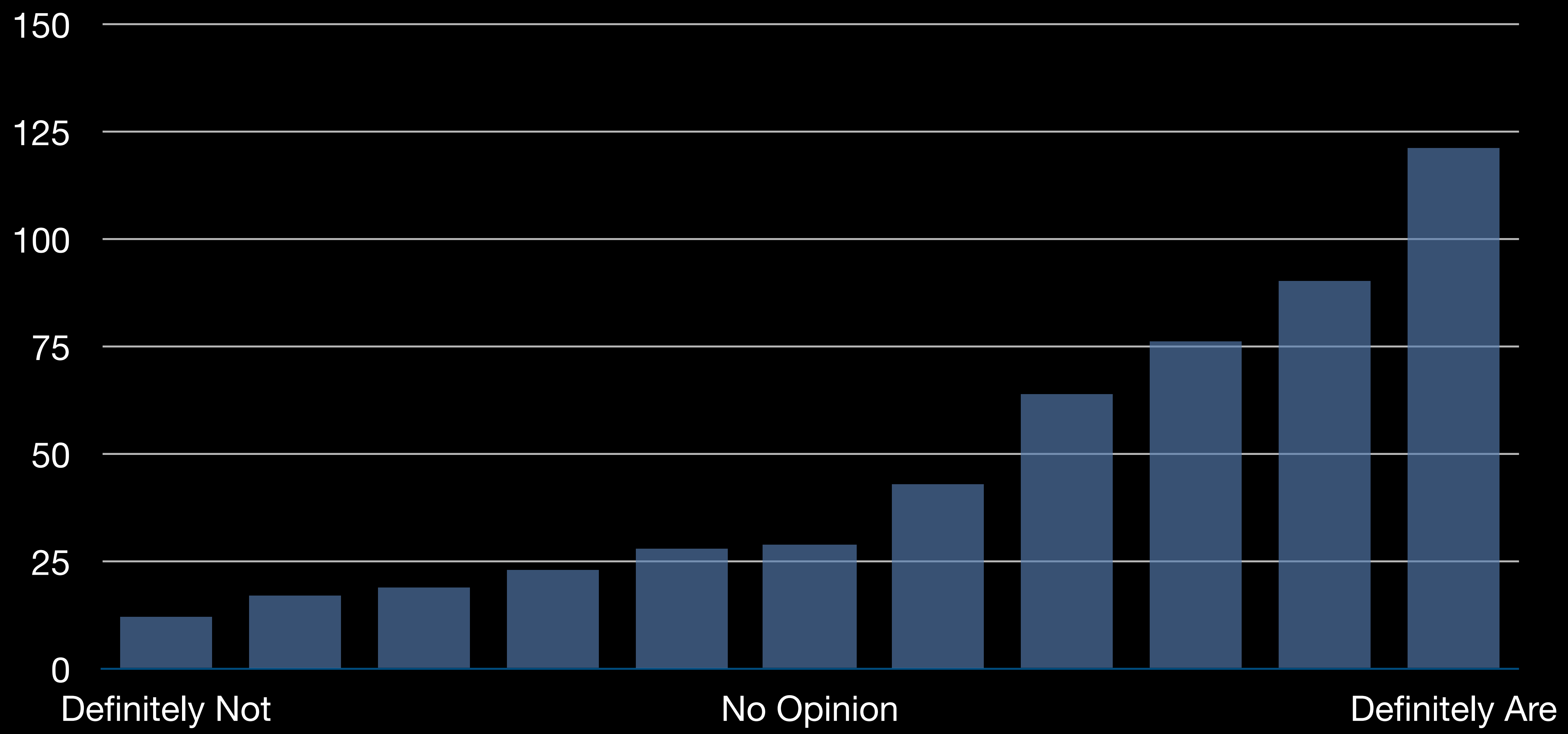
Health Care



IT and communications systems related to health and medicine. This includes the online systems of medical services and clinics, medical telecommunication (telemedicine, ambulance medical telemetry, etc.), sources of public health information, pharmaceutical production and distribution, health and drug regulatory and oversight systems, and health insurance IT systems.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

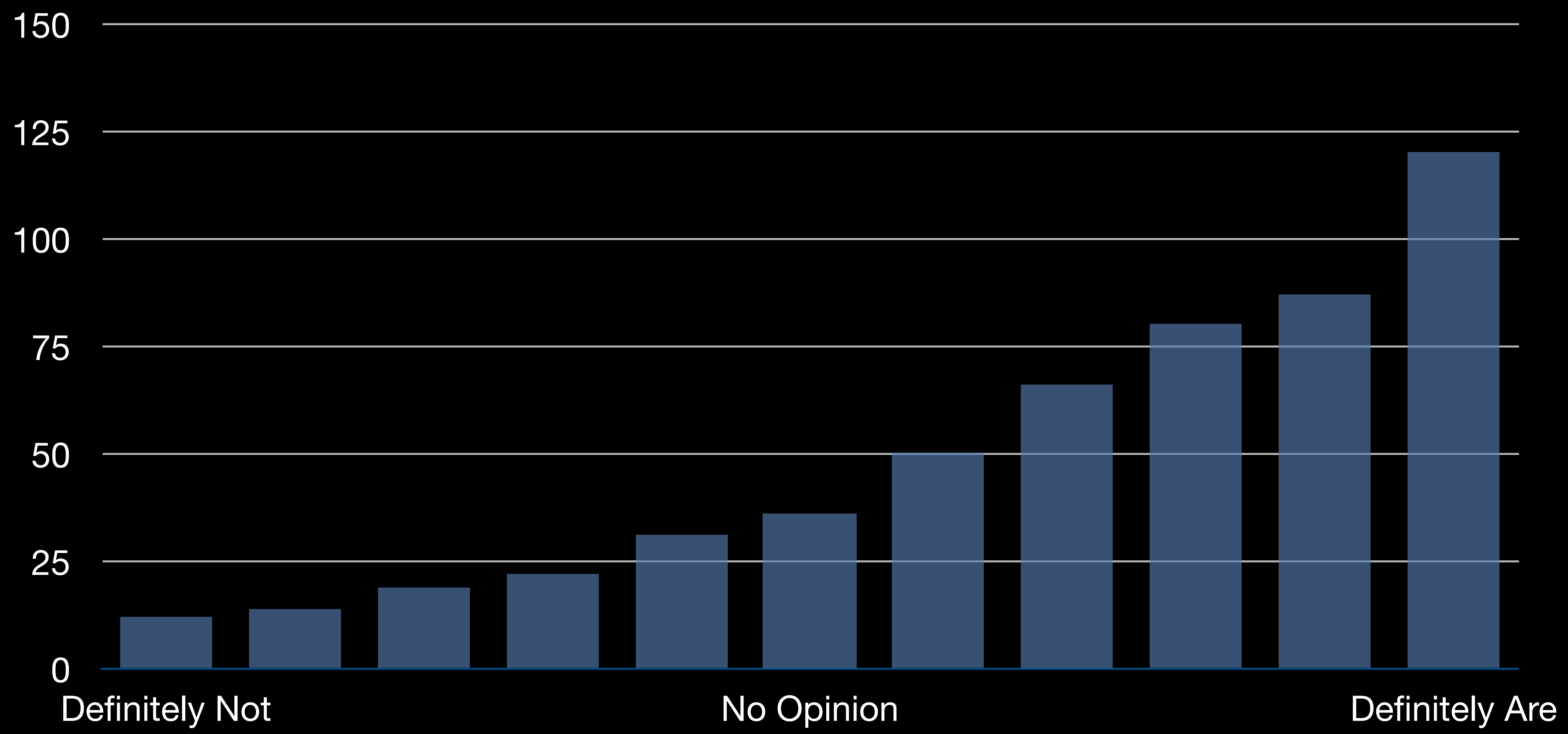
Food Supply



Systems related to agricultural production and the food distribution chain, including crop and farm management SCADA/DCS systems.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Education



Systems related to educational facilities and institutions, including child-care and pre-school facilities, schools, and civilian higher education and graduate level academia.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Internet Infrastructures

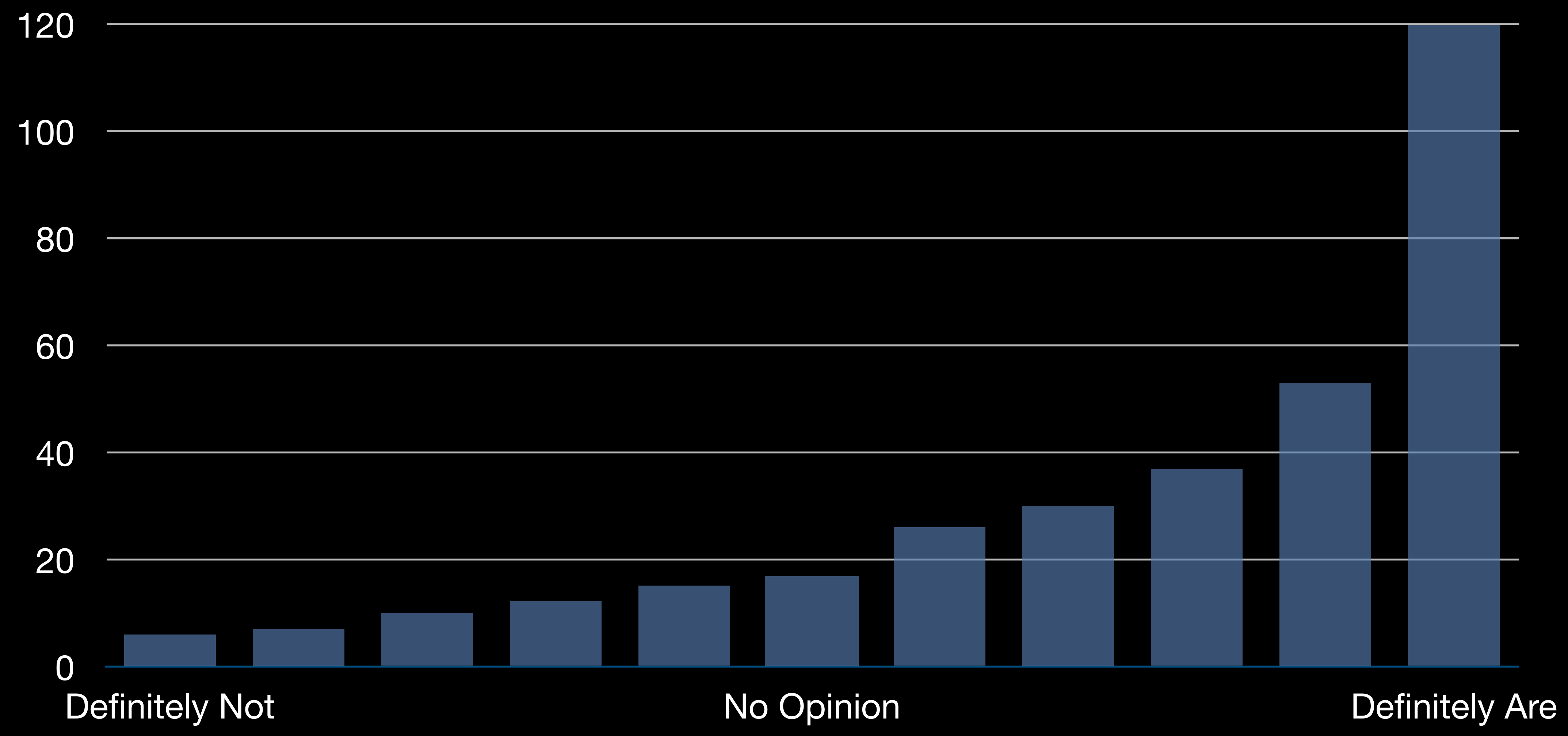
Consider systems that are part of the Internet communications infrastructure itself.

Again, in all cases, we are discussing civilian infrastructure and in some cases dual-use infrastructure, but not military infrastructure.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Naming & Numbering

Domain Name System

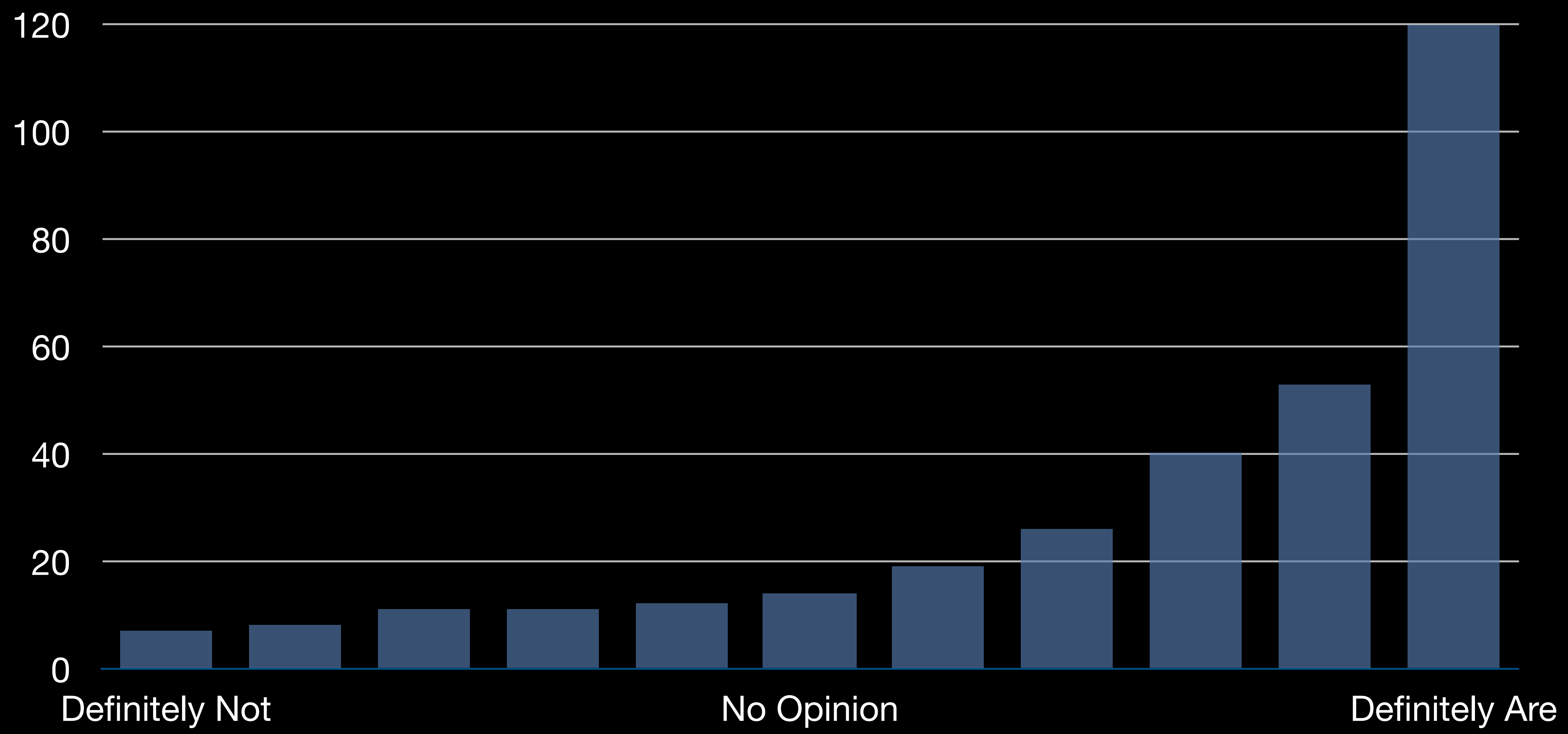


Systems and data used for the operation of the Internet's Domain Name System (DNS). This includes root name servers, the content of the root zone, and the IN-ADDR hierarchy for reverse DNS lookups, DNS infrastructure and processes used to sign DNS records for authentication (DNSSEC), name servers and zone content for country-code, geographic, and internationalized (non-ASCII character) top level domains and for new generic and non-military generic top-level domains. This also includes frequently used public recursive DNS resolvers.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Routing & Forwarding

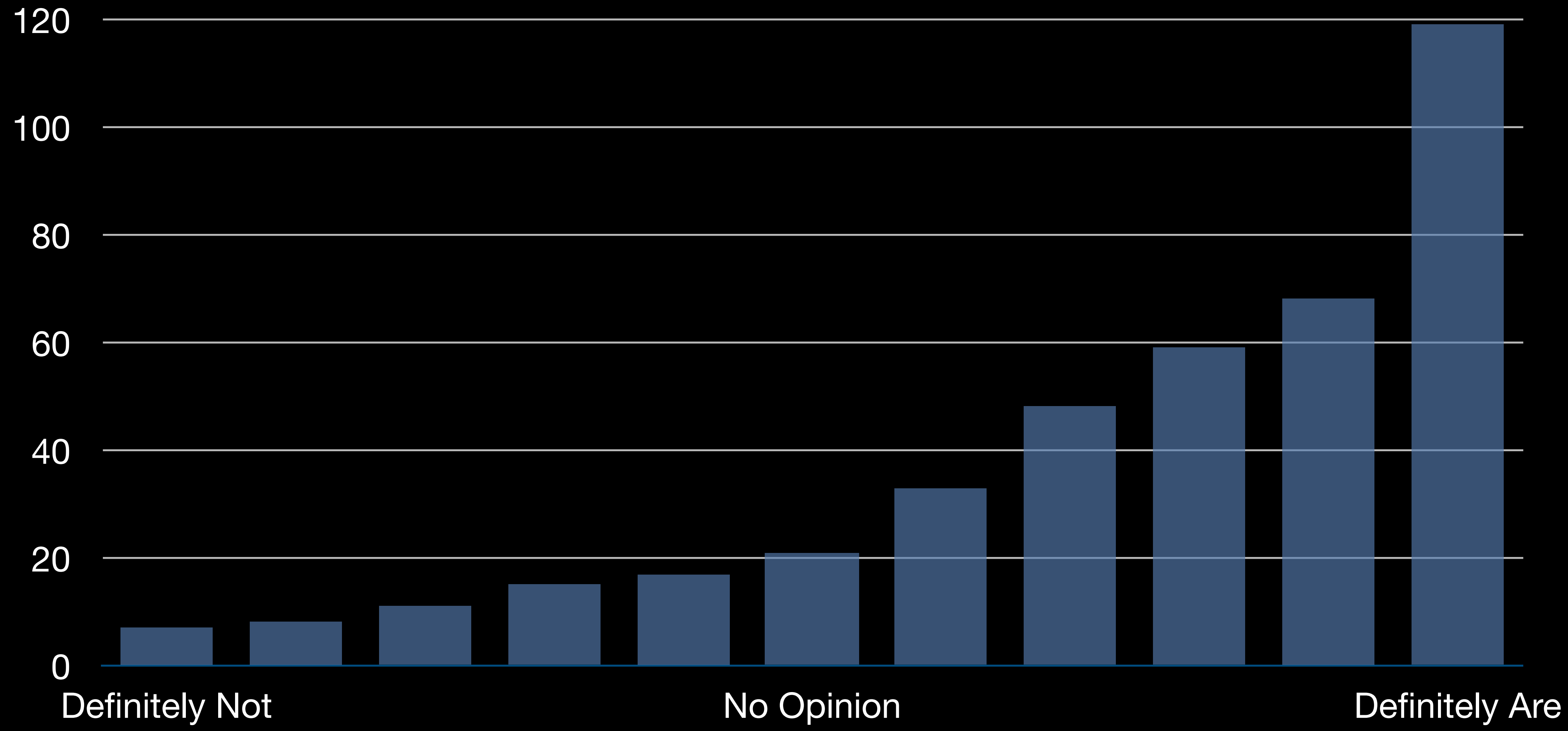
Routing



Equipment, facilities, and databases used in routing of packetized IP communications over the Internet. This includes both core and peering routers of major networks, Internet forwarding systems, physical sites where networks interconnect (Internet Exchange Points), systems that assure routing authenticity, public routing registries (RADB, IRRs of Regional Internet Registries, and systems for defensive routing of attack traffic (Real-time blackhole RTBH routing services). This also includes the routing protocols themselves and the integrity of the IETF processes and outcomes for protocol development.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

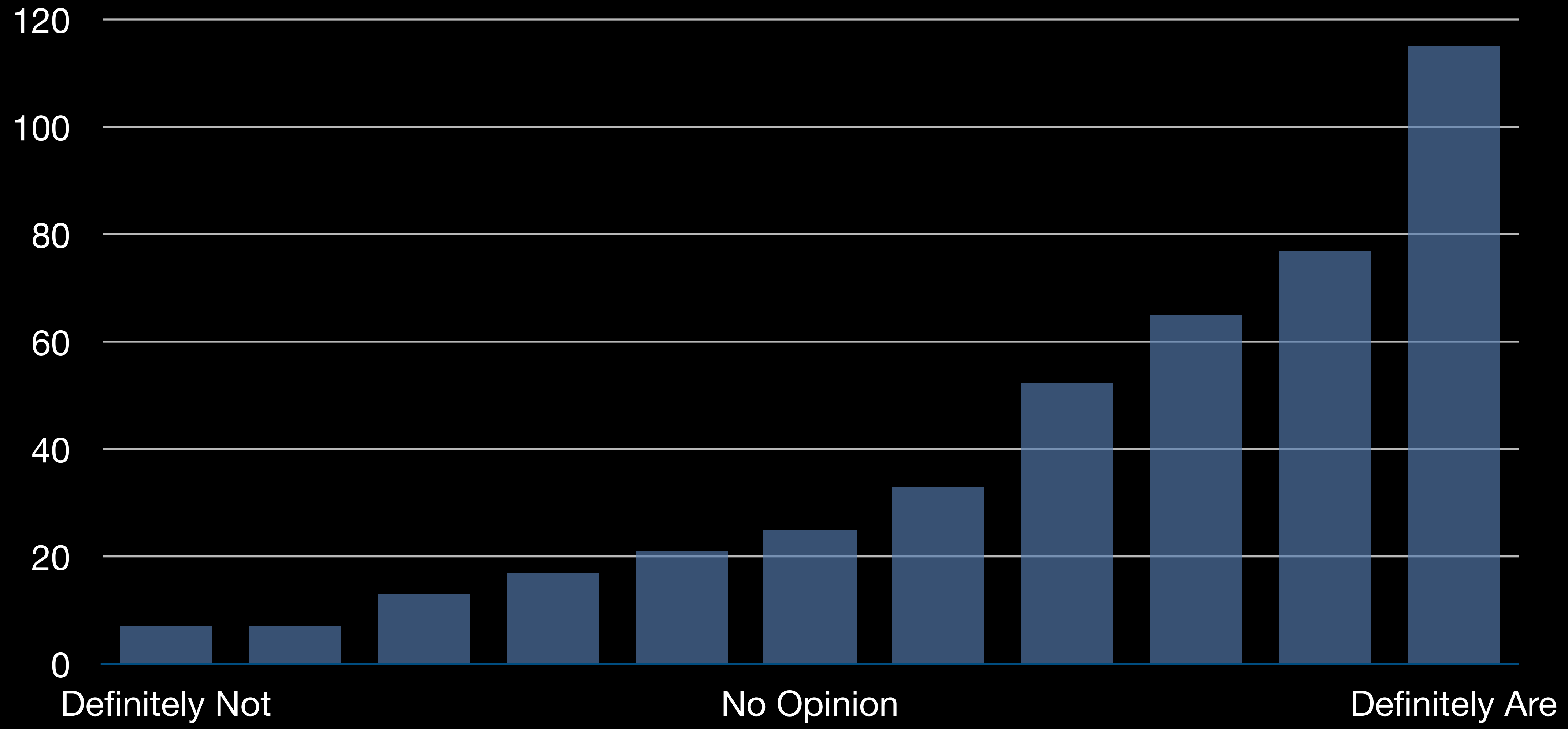
Cables



Physical cable systems and installations for wired communications. This includes high capacity trunk lines and landing stations for undersea cables serving multiple regional cable systems, fiber optic cable systems that individually serve regions or provide redundant communications paths for large populations, and wired infrastructure for cable television.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Wireless

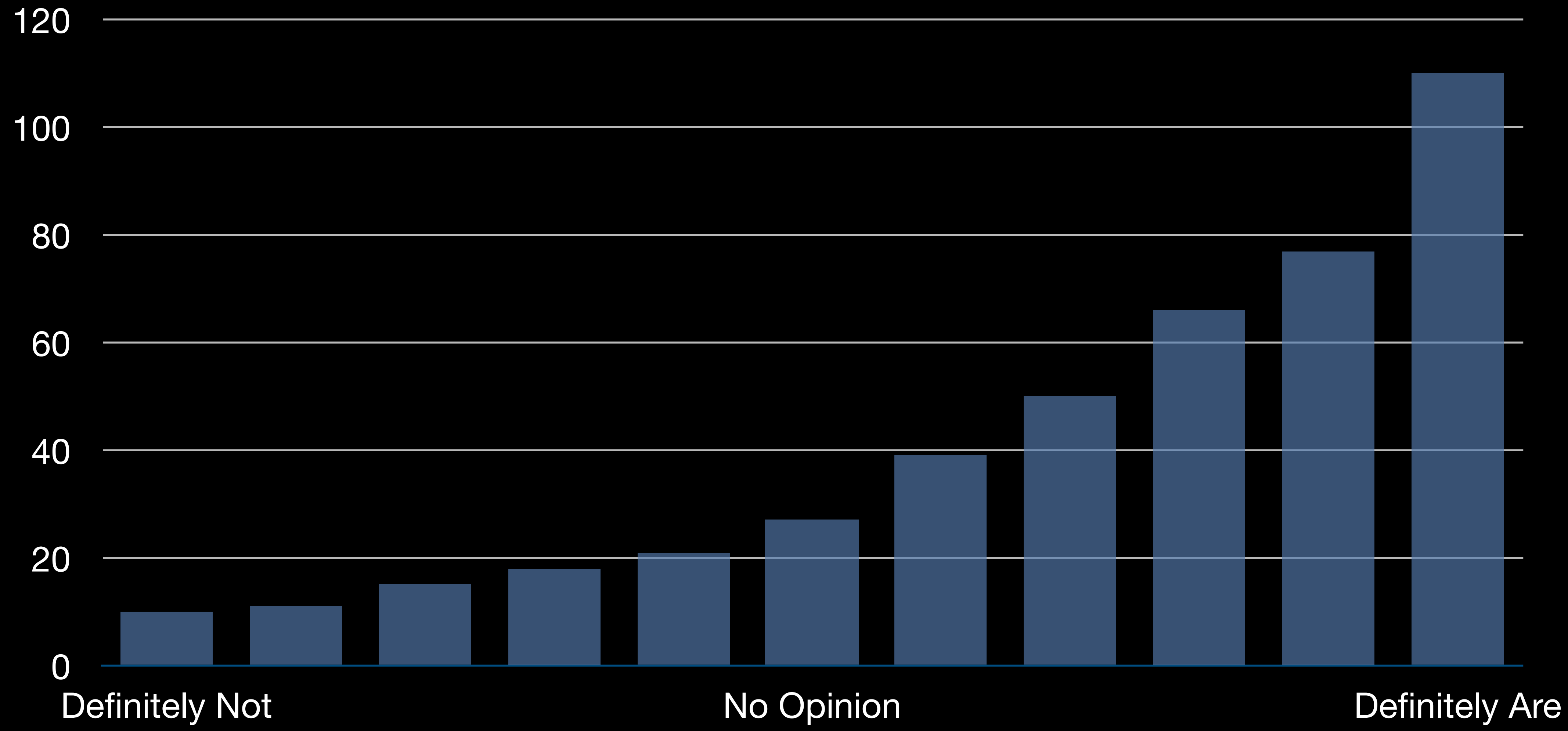


Infrastructure and systems for wireless communications. This includes back-end 4G/5G infrastructure for cellular communications, as well as regulated and unregulated broadcast communications carriers.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Supporting Infrastructure

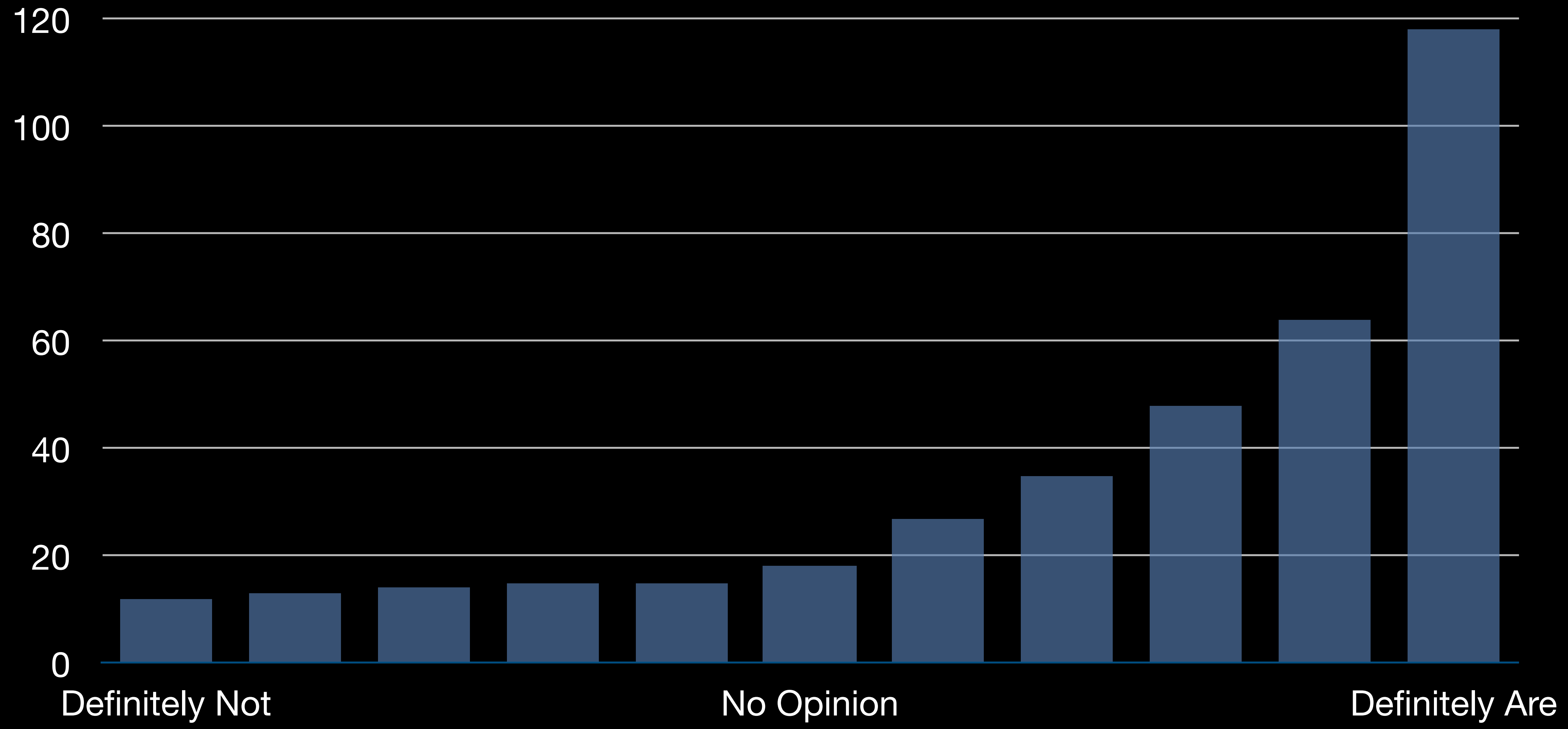
Datacenters



The operational and safety systems of server-hosting datacenters.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

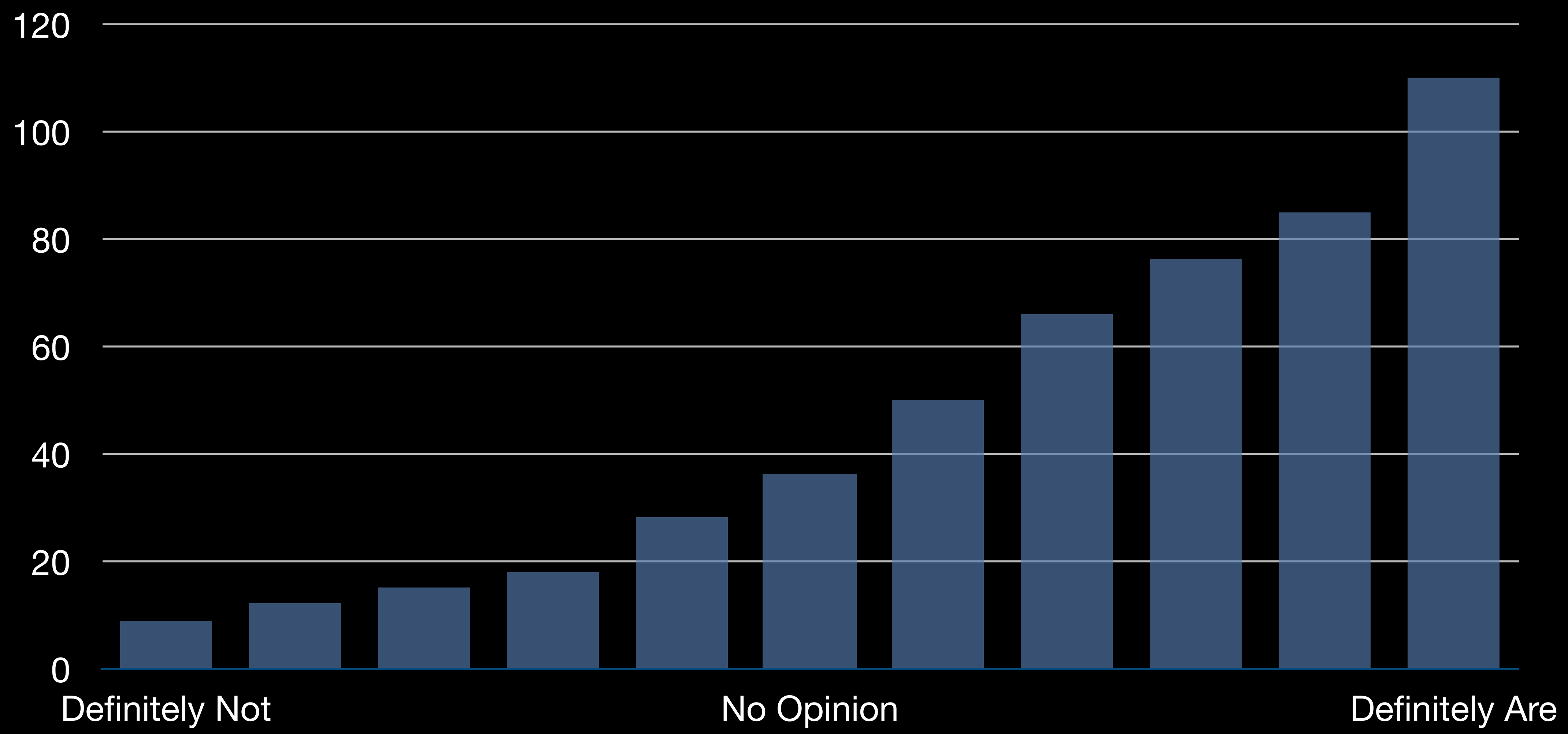
Certificates & Trust



The management of cryptographic keys which are used to authenticate users and make Internet transactions like web browsing and email secure and private. This includes things like SKS and other PGP keyservers, legacy Certificate Authorities and their Public Key Infrastructure, and certificate revocation mechanisms. Also, mechanisms like password managers (1Password, LastPass, iCloud Keychain), WiFi roaming authenticators (Boingo, iPass), and social-media authentication services (“use Facebook, Twitter, Google, or LinkedIn to login”). Also, spam and malware blacklists and whitelists and the threat intelligence services that produce them.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

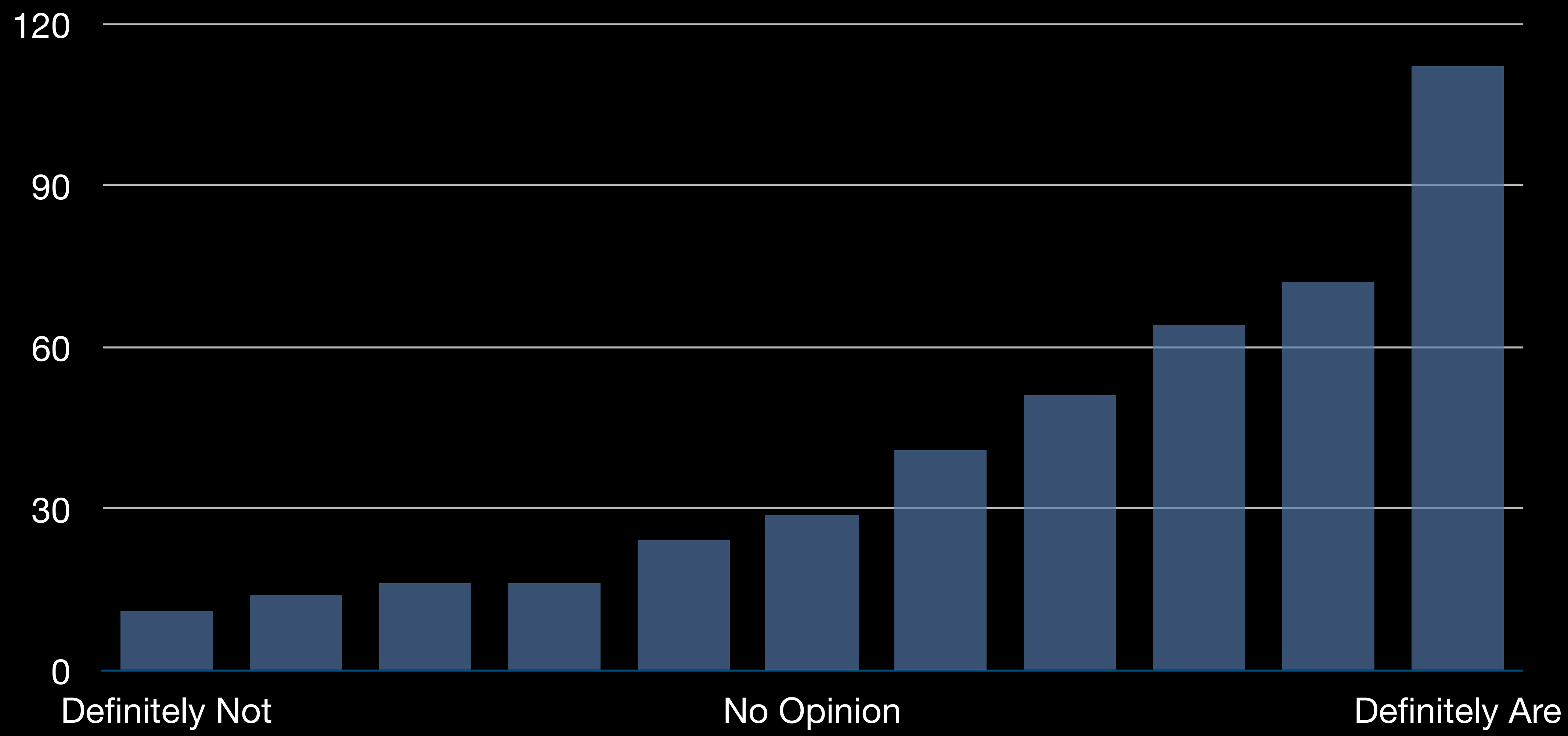
Mapping



Systems which provide geographic mapping information and services to the public for navigation and other purposes, for instance OpenStreetMap, and MapQuest, or provide geolocation information to industry, like MaxMind and Quova.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

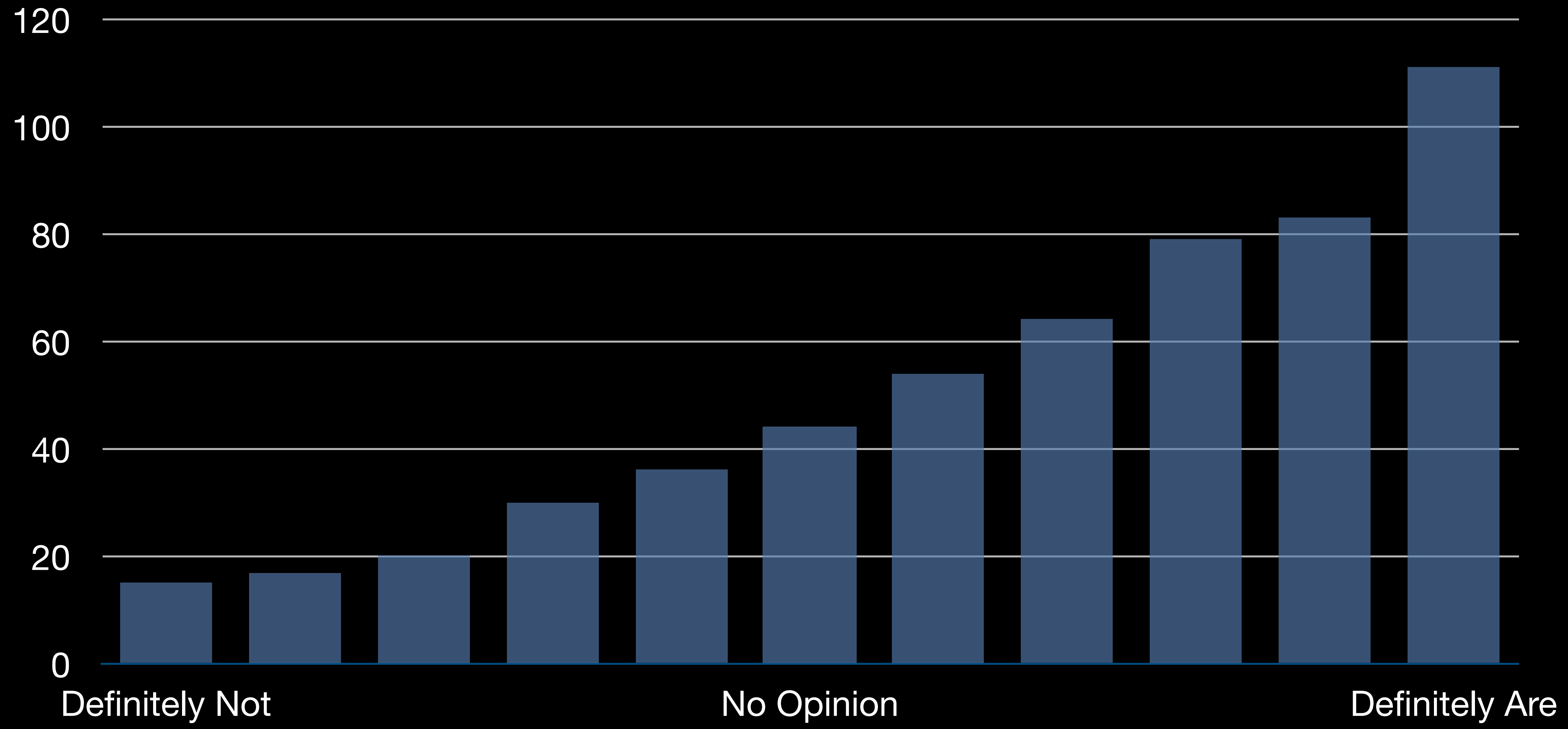
Software



The availability and integrity of the source code and patch-distribution infrastructure of software used in the core of the Internet, and by large portions of the Internet-using public. For instance, widely-used operating systems and compilers, common DNS servers, mail transport, delivery, and user agents, web servers and browsers. Also automatic patch distribution systems (Apple Update, Windows Update, BigFix, etc.) and the software update processes for SCADA, embedded systems, and IoT devices.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Cloud Services

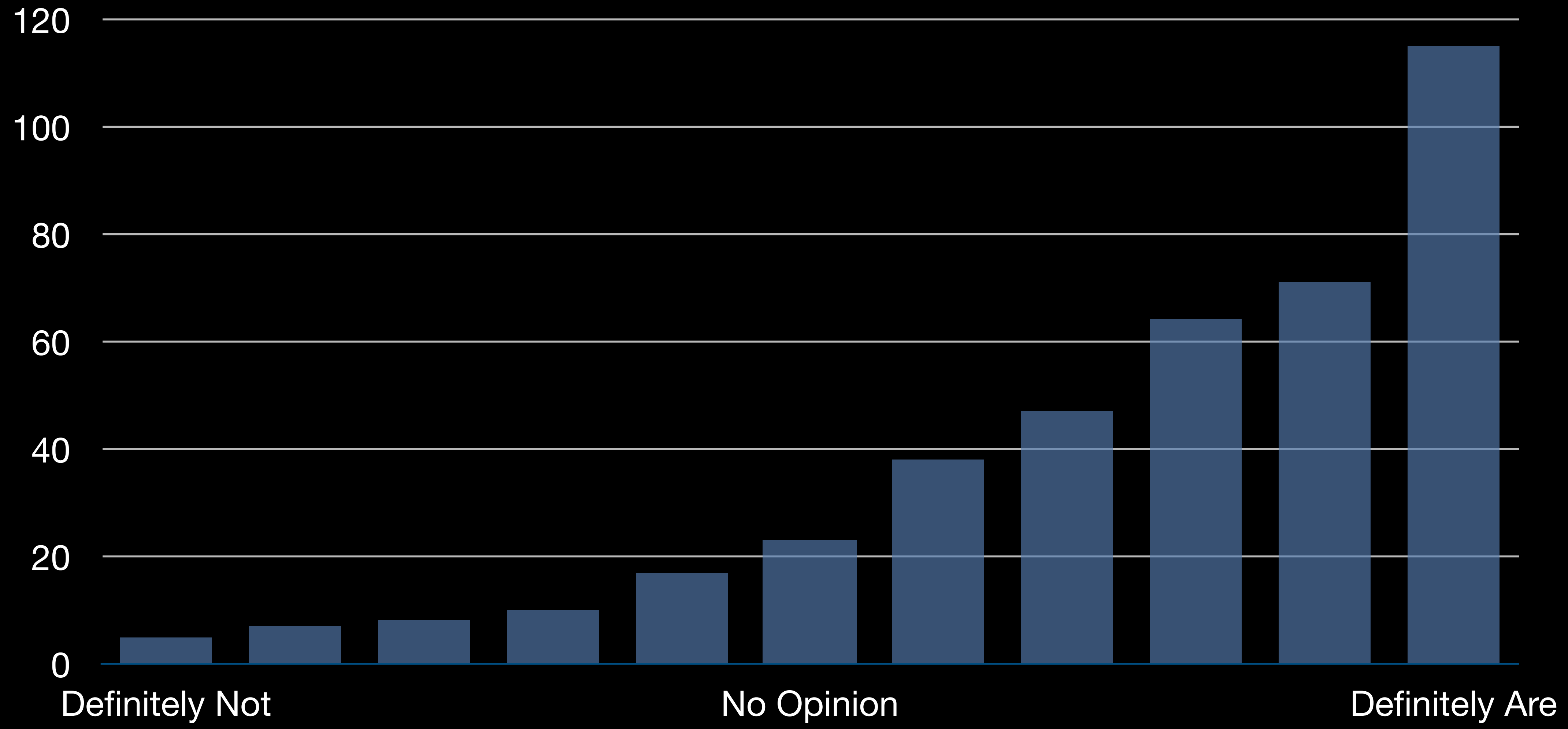


The infrastructure which makes “cloud” services possible, including cloud service platforms like Amazon Web Services and Microsoft Azure.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Services

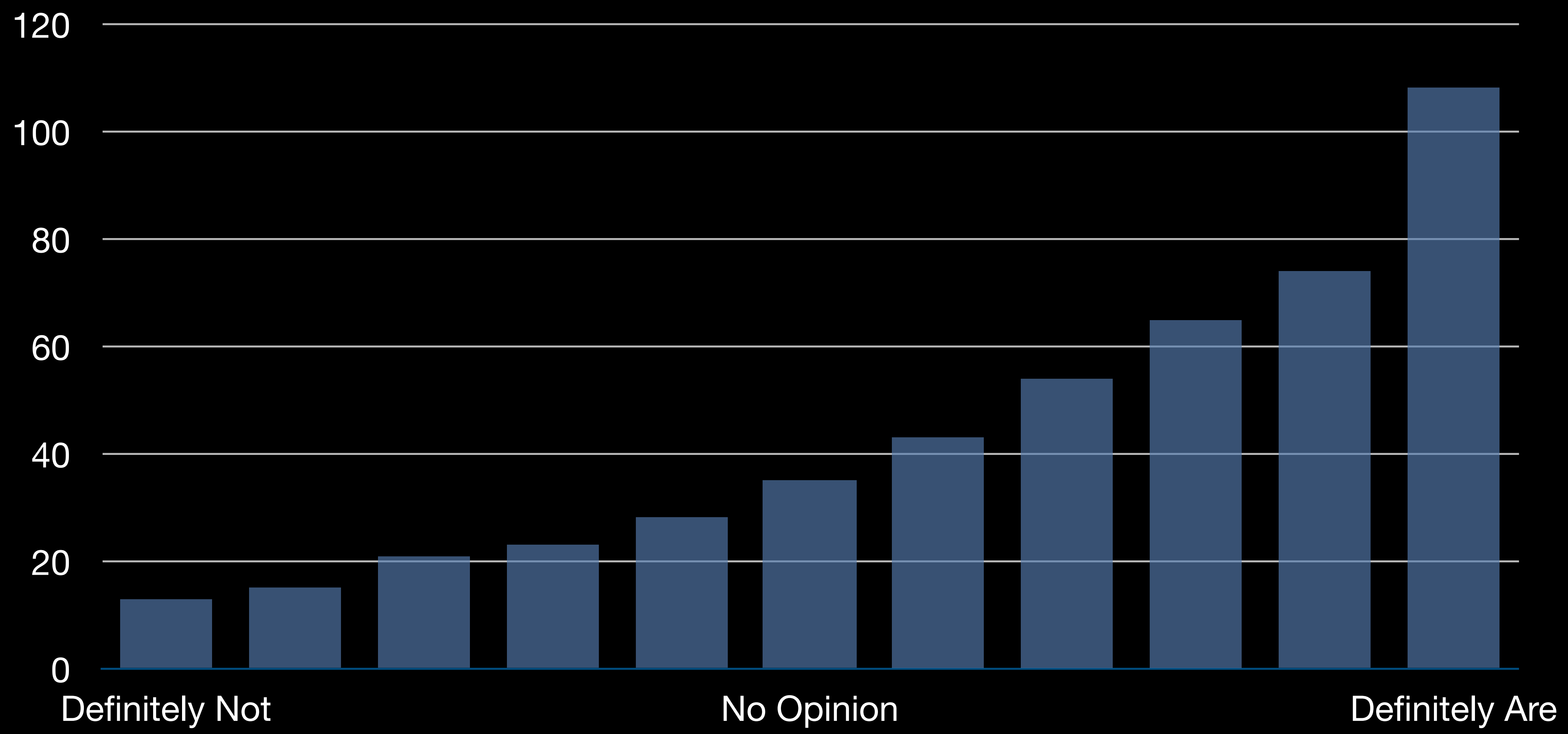
Financial Transactions



Internet-enabled banking, such as the web sites online banking facilities of retail banks, and payment systems like Stripe, Paypal, and Apple Pay.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

World Wide Web

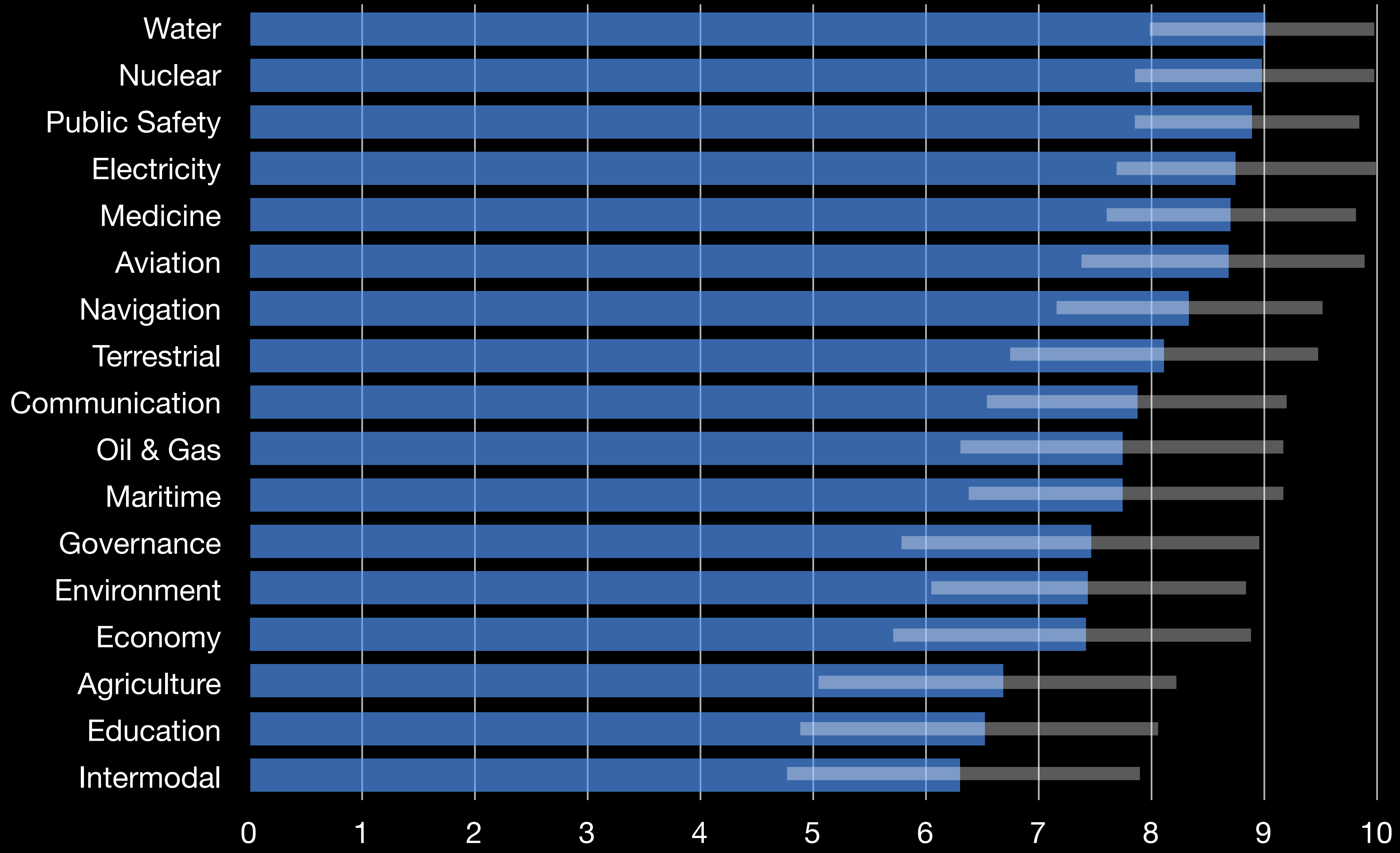


The network infrastructure that enables web browsing, including search engines (Bing, Yandex, DuckDuckGo, Google, Baidu) and content distribution networks (CDNs) like Akamai, Limelight, Cloudflare, and Cloudfront.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

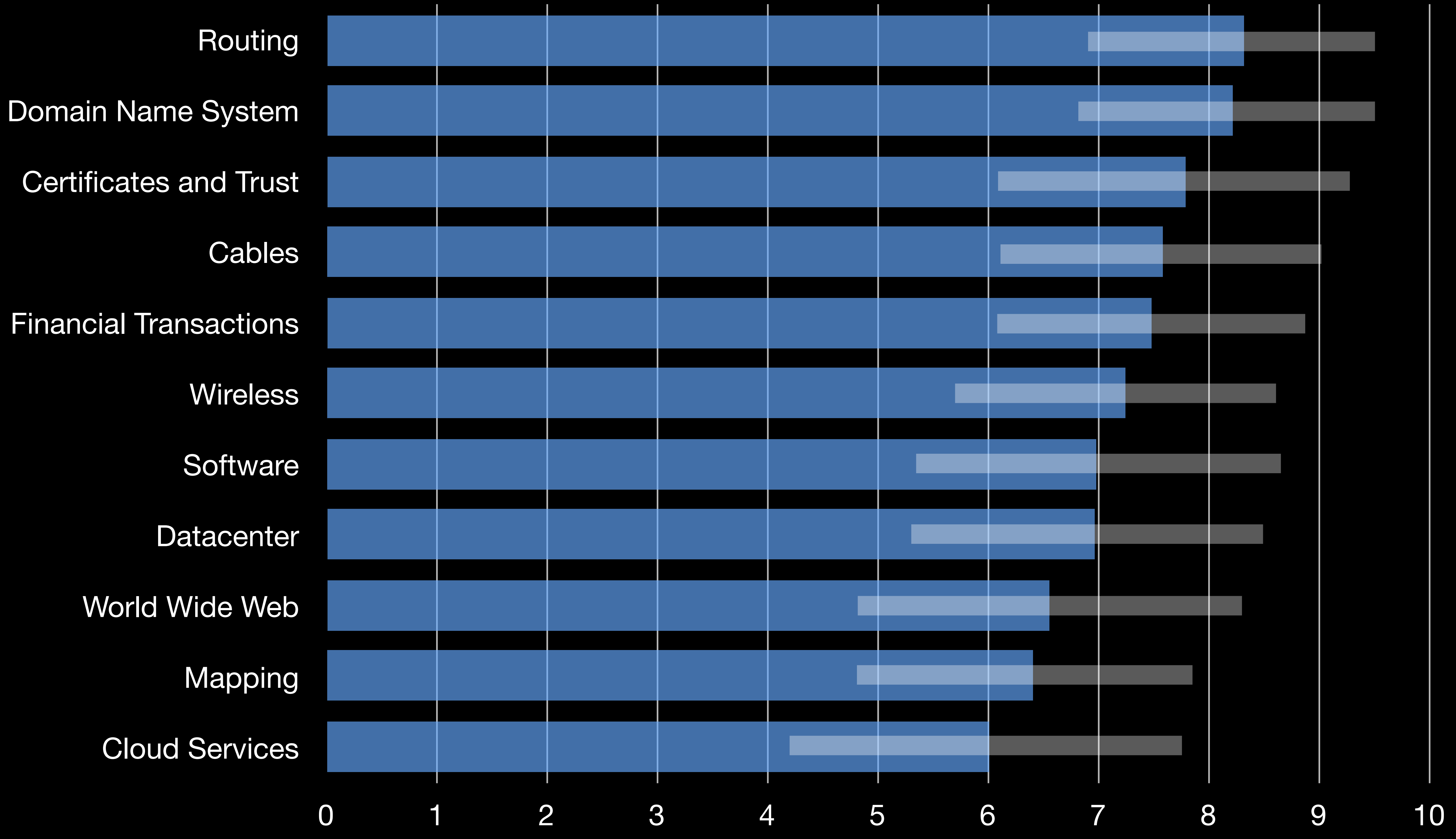
In Summary

Traditional Infrastructures



This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Internet Infrastructures



This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Respondents' Comments

Security and protection is a wide topic. I feel it wasn’t clear on the jurisdiction of who actually does the protection.

As Governments usually makes laws and policies and form an organ to enforce such, then who actually implements?

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

A majority of the infrastructure we use every day is still built on obsolete technology and is more fragile than it should be. If there is a common understanding that this infrastructure is vulnerable and it is seen as a legitimate target to attack, this would change how we use and deploy infrastructure.

I am thinking especially about banking and money transfer (move towards blockchains, or IOTA based solutions), encryption and site security, decentralized Internet (perhaps moving towards IPFS kind of solutions), decentralized clouds, better and more secure routing solutions.

The current trend to centralize more and more parts of the Internet makes all communication based on it more vulnerable. This trend must change.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Answering without understanding the cost tradeoffs misses a dimension. Hard to include that in the survey, though.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Defending against criminal actors is hard enough. Now we have to deal with potential attacks from state sponsored actors. Electronic attacks on civilian infrastructure could potentially kill thousands of people without warning, so I'd like to see international protocols in place to help prevent that.

In my opinion, potentially lethal cyberattacks should be as far beyond the pale as using a nuke.

There's a flip side to legal protections though—although international law may protect a potential infrastructure target, the operators of that infrastructure *must* do everything in their power to secure it properly, and must be held accountable or liable if they fail.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

I feel strongly that in some of the categories there is a need for a finer grained break-down.

For example, the question in regards to crypto, certificates and passwords groups together GPG/PGP key services and also commercial password managers like 1Password. These are quite different in their usage, target end-user group and also criticality. I do not see any need to offer any special protection to password management tools. The decent ones usually have offline sync, making a cyber attack against their cloud infrastructure, while inconvenient, still largely mitigable, in many, if not most cases.

On the other hand, volunteer run GPG key distribution is at higher risk, and of larger impact that is more difficult to mitigate, and should be afforded protection.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

If military type action (cyber, conventional, or nuclear) has been decided to be undertaken by a country, then most things are open to attack except water supplies and healthcare services in my opinion. Some more than others, perhaps.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Now that everything is going digital, security is paramount.

I do not see any sector that does not critically need protection.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

believe there should be a clear differentiation of systems which provide for requirements for human life. Water and medical systems are mentioned specifically, but any systems required to sustain life should be in a special category of protection, which should go above and beyond things like “cloud services,” if the latter is sought to be protected.

By placing various non-critical services in the same category as water and sewage treatment and other critical infrastructure to sustain human life and health, we devalue protections on the latter.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

This is a gigantic waste of effort. Asking hostile countries to not attack certain infrastructure is like posting signs saying “Please do not burglarize my house.” The hostile entities won’t care that the signs are present, and certainly won’t agree to be bound by the terms laid out. Internet security is the responsibility of those deploying the infrastructure, not those who would attack it.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

I believe the stability of cyberspace to be extremely nuanced and consider these surveys to be somewhat misleading given the risk of miscalculating networked cascade effects in context. I feel that there may be hidden assumptions that could be surfaced more outright. e.g. the survey appears to focus on the causal effects singularly, and not their combinatorial or multiplier effects over time. Assume that everything's digitally connected and work back from there. Whether one infrastructure is more critical than another depends on their cascade relationships and consequential effects, and those depend greatly on the level of socio-economic development and interdependence of digital systems. I am concerned that the work of the GCSC may be focusing on the wrong "end" of the problem. Ironically perhaps more progress can be made by not focusing on the "prevention" side of the equation, a natural starting point, but more contextually on the "cure" side of things. I understand that this approach might appear to be a back-to-front analysis—rather it is a back-to-business analysis.

Specifically, what infrastructure must remain functional if digital society is to have the most humane and reasonable chance of "bouncing back" in less than half a generation?

Hence my consistent emphasis on digital archival sources, cultural and historical libraries being "out of bounds." These are critical infrastructure if, ex-post-facto, society is going to bounce back in a meaningful and socially stable way. A functional "one-of-everything" definition is a simplistic model, but perhaps useful starting point for discussion.

Lastly, I preferred the earlier survey as you may now be simplifying the questions to the point of it losing resolving power in the responses. Everything risks being considered critical by someone, given their interconnectedness and different stages of development, so you risk being back at square one. While I understand the desire to gain quick feedback, lists are one dimensional. You only really know whether an infrastructure is indeed systemically critical after it's gone and you find yourself unable to rebuild.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Individual social media companies and other market-based organizations must be responsible for their own security.

Public infrastructure that provide the basics of life should be untouchable.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

If you receive responses that slide any of these sectors into a negative (not important) position, there is something seriously wrong with the general public’s understanding of critical infrastructure.

Governments had better set out immediate remedial education plans.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

In a data-driven economy, almost every sector will (with varying degrees of speed) become unable to function if its digital functions/infrastructure are unavailable or unreliable. For example, when automated rail signaling systems fail, reverting to manual signaling effectively cripples the service (even though originally, all rail services ran on the basis of manual signaling). However, the last two years suggest that information infrastructure can be attacked in much more subtle ways (than simply knocking it out of action), and yet see significant damage.

The phenomena of “fake news”, Twitter bots, voter analytics at the mass scale, and targeted campaigning/advertising appear to have had a quantifiable effect on more than one recent democratic process. One way to interpret this is as an attack on the “integrity of the information infrastructure.” The solution is not clear. According to Gresham's Law, “bad money drives out good.” “Bad” information achieves both reach and traction far more easily in the data-driven economy than it used to be able to. In totalitarian states, the state controls the dissemination of all information to the public; in the data-driven economy, any civilian can self-publish (“samizdat”), but it is also possible to swamp the genuine and factual opinions of well-intentioned individuals with false/untrue information that can sway public opinion as a whole (or at least, a critical mass of it).

This may not, strictly speaking, be a flaw in the infrastructure, but rather, a consequence of how a general-purpose and generally-available information infrastructure can be used and abused. More repressive states are already responding to this threat by trying to increase state control of how the general-purpose infrastructure may permissibly be used. That is more likely to do harm to well-intentioned users, and to the health of the infrastructure and society as a whole, than it is to effectively inhibit the spread of information that such states wish to suppress.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Depending on the city, hotels, churches and metro locations should fall within the scope of “critical infrastructure.” These are sometimes the only places where people can stay safe for a longer period of time. A “security and safety” map of a city would help to identify such locations.

Building a hierarchy is important, as is taking the factor of time into consideration. Not all critical infrastructure objects are critical within the first hours of a serious attack (for example).

Second, born out of experience (Mumbai attack in 2008): keep the Internet infrastructure alive even if it might help terrorists. It helps victims to survive.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Many of the questions needed an “it depends” option—for most of the questions in which I answered “no opinion,” I meant that some of the resources mentioned may be critical, but not all, and it depends how they are viewed. Many of them are designed with a redundant distributed architecture, so any one instance of the resource is not critical, but as a class they may be.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License

Great job!

I think that *all* of the infrastructure you mention *is* critical infrastructure, and *all* of it should be protected regardless.

This document is published under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) License