mozilla

Mozilla Cybersecurity Delphi 1.0: Towards a user-centric policy framework

Table of contents

Executive summary 3

What is a Delphi study & who participated 5

Agreeing on terms: defining cybersecurity 8

Users, tech & norms: A broad picture of issues & levers in cybersecurity 11

The user environment 12

The technological environment 14

The normative environment 16

Cryptography, information sharing, and the protection of critical infrastructure 18

The elephants of cybersecurity policy 19

A way forward: towards a user-centric and holistic approach to cybersecurity policy 21

Appendix A: Policy list 23

Appendix B: Weighted scatterplot of all suggestions 25

Appendix C: Participant engagement 26

Appendix D: Participant bios 27

Executive summary

From compromises of some of the world's largest corporations, to critical vulnerabilities in widely used open source software, to exponential growth in the number of connected devices and users, the need to proactively design policies and practices to secure users and Internet infrastructure has never been greater. Yet, cybersecurity public policy conversations too often are siloed and grounded in a few old ideas that don't encompass the totality of the threat landscape. As a result, the state of cybersecurity policy today does not have a compelling answer for global-scale vulnerabilities like Heartbleed or nation-state attacks on public and private sector actors. The concern for cybersecurity from all stakeholders has only been growing, but cybersecurity policy remains a broad and contested field lacking clarity on the best paths forward.

To help cut through the rhetoric and identify consensus on areas of cybersecurity policy that should be prioritized for further attention and investment, Mozilla brought together more than thirty leading cybersecurity experts from a wide variety of backgrounds: academia, civil liberties, government and military, security, and technology.

Amid a plethora of definitions of cybersecurity, often leading to different policy and practical interventions, our participants converged on the essential technical core: the confidentiality, integrity, and availability of information. An immediate implication of this finding is that traditional government cybersecurity paradigms that focus heavily on securing critical infrastructure should shift and expand to consider a much wider array of connected users and devices, types of actors, and types of risk. Framing this definition properly also matters: our participants noted that elements of human rights (especially privacy) and economics belong at the core of a balanced and comprehensive view of cybersecurity.

Focusing on users and securing their experience online is a critical part of this expanded understanding of cybersecurity. Much can be done to help the average person make the right security choices, but our participants also identified the need to automate security and enable security by default as much as possible. For instance, in the case of cryptography, four times as many experts wanted to make tools easier or automatic for the average person, as opposed to solutions oriented towards teaching people about cryptography and how to use encryption tools.

Participants repeatedly highlighted the state of cryptography as an area requiring more attention and priority, and pointed specifically to such needs as: increasing the ubiquity of cryptography, making secure cryptographic tools easier to use, strengthening the integrity of public key infrastructure, as well as developing and deploying alternative means of authentication other than passwords. Our experts found a number of such objectives to be highly desirable, but not necessarily feasible (and vice versa). However, one recommendation for government action that stood out above the others as both highly desirable and highly feasible was greater funding to maintain the security of free and open source software.

Building norms for acceptable behavior online was also a popular priority for government action in cybersecurity, and to our surprise, arose in all segments of the panel. Participants felt that cybersecurity norms should apply to governments as well as to others stakeholders, and noted that corporations should be concerned about and involved in normative development efforts. Again, framing is important: our experts noted that human rights should guide the building of cybersecurity norms, and norms should be communicated and shared clearly and openly in the international arena.

Cybersecurity conversations are often dominated by three specific topics: cryptography, information sharing, and critical infrastructure. We call these the "cyberelephants" – the well chartered waters of the issue, and oldest and most common topics of governmental conversations on cybersecurity. Privacy-respecting information sharing policies, efficacious critical infrastructure protection, and widespread availability and understanding of secure encryption programs are all hard goals to achieve despite their critical importance for the state of security in the digital world. This is why those issues are ranked high on desirability despite their implementation challenges. Yet, throughout this study we found that the focus on these "cyberelephants" tended to obfuscate the other levers, problems, and priorities in cybersecurity policy that merit further attention and investment, many of which we've already identified here.

A closing word on the study's research methodology: in order to identify consensus across our experts' different backgrounds and expertise, and to encourage more constructive approaches, we created a tailored methodology based on the Delphi method. The Delphi method, originally developed by the RAND Corporation in the 1950s, engages experts throughout iterative rounds of pseudonymous contributions. Pseudonymity encourages good ideas to succeed on their merits, stripping them from reputational effects and force of personality.

Through a multistage process including three rounds of surveys and intermediary online discussions, the Mozilla Cybersecurity Delphi Project improved our understanding of the different perspectives and priorities in cybersecurity policy, helped us identify where consensus could emerge and where conversations are likely to get stuck, and generated a list of 36 policy suggestions (see Appendix A) using a variety of approaches and levers including legal tools, new laws and regulations, technological fixes, and research. This report summarizes the insights from this study, but it is not an exhaustive report on all cybersecurity issues. Rather, it is meant to be a first step towards a more open, holistic, and collaborative policy conversation.

Many thanks to our expert participants and research team for helping to improve our understanding of the cybersecurity policy landscape, which we hope will lead to a more informed global public debate.

What is a Delphi study & who participated

The Mozilla Cybersecurity Delphi engaged a group of cybersecurity experts from diverse backgrounds to discuss the state of cybersecurity policy and identify areas of consensus on policies and practices that warrant priority in the global debate and further investment.

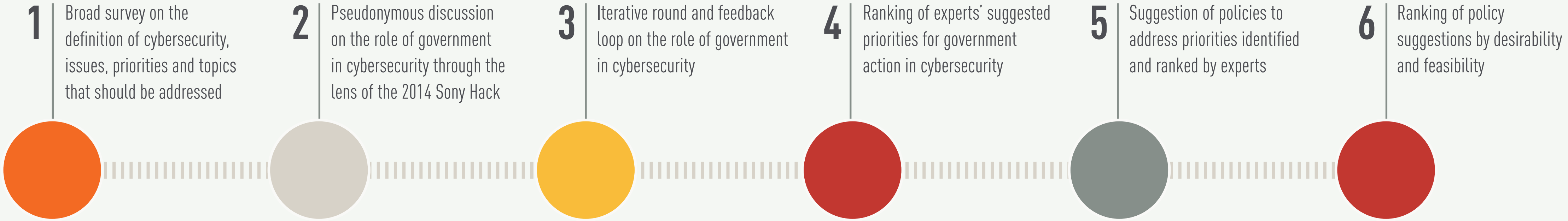
What is a Delphi?

The Delphi method is an iterative process (repeated in multiple steps) usually involving a group of experts to reach consensus on a complex issue. It is an effective method when experts are likely to come from different perspectives and to disagree based on their backgrounds and localized sets of priorities. The technique uses a pseudonymous format that encourages more candid feedback, allows all individuals in the group to speak freely, without judgment, and gives equal weight to each individual's opinion based on its merits rather than lending undue influence to verbal or physical presence or the reputation of the speaker. The objective is to reach some degrees of consensus through a process of identifying common opinions among the group.

Has this been done before, and what are the key steps?

The Mozilla Cybersecurity Delphi Project is the first study that we know of to undertake a Delphi-inspired process to tackle cybersecurity issues. Three online surveys form the backbone of the Mozilla Cybersecurity Delphi, each accompanied by rounds of participatory discussion allowing experts to engage each other on earlier findings and to reflect on the shared responses. The iterative nature of the process provides experts with opportunities to validate their responses or to shift perspectives and priorities based on comments and aggregated feedback from others on the panel. A key element of the study was to engage participants with different perspectives arising from different "segments" (i.e., academia, civil liberties, government & military, security, and technology), including some that may have opposing views on cybersecurity issues and solutions. Another important element was transparency of the process. To this end, there was little to no elimination or combining of priorities or suggestions. Throughout the research process, participants engaged with long and diverse lists of issues, wide-ranging comments, opinions, and information. The multistage process of expert engagement included the steps below:

Delphi process



1 Broad survey on the definition of cybersecurity, issues, priorities and topics that should be addressed

2 Pseudonymous discussion on the role of government in cybersecurity through the lens of the 2014 Sony Hack

3 Iterative round and feedback loop on the role of government in cybersecurity

4 Ranking of experts' suggested priorities for government action in cybersecurity

5 Suggestion of policies to address priorities identified and ranked by experts

6 Ranking of policy suggestions by desirability and feasibility

How did the project start, and what were participants asked to do?

The first step was open in nature and included asking the expert panel 17 open-ended questions about their understanding of cybersecurity as well as the policy levers and priorities for a more secure digital world. This served as the foundation for soliciting both broad and specific information about the definition of cybersecurity, the role of government in cybersecurity, current vulnerabilities, and perceived threats. Our experts elaborated on what changes to individual computer systems would have the biggest impact on cybersecurity, whether they believe government should or should not be involved in certain areas, what cybersecurity topic gets too much or not enough attention, etc. A follow-up step framed the responses into a list of core issues, where experts were asked to review the summarized items, provide feedback and/or adjust their responses and priorities, and to rate the list of issues with an eye toward cybersecurity policy suggestions or ideas. At this point, outcomes and priorities began forming, leading to a long list of policy suggestions developed by our panel. Again, participants had an opportunity to provide feedback and add to the list. The final step asked the experts to rank the full list of cybersecurity policy suggestions based on desirability and feasibility.

What are the limits of a Delphi method?

This initiative is not meant to be a comprehensive study of all cyber related policy issues, or to fully represent the various industry segments in the study or the diversity of expert opinions in the space, but rather to build some level of expert consensus using an open and multistage process. And since there is no “standard” number for what constitutes an adequate sample for Delphi, it is often difficult to determine what size is acceptable for a panel, or for any analysis. The Mozilla Cybersecurity Delphi process was time consuming as we moved throughout the iterative stage and we are truly grateful for the continuous engagement and participation of all our participants.

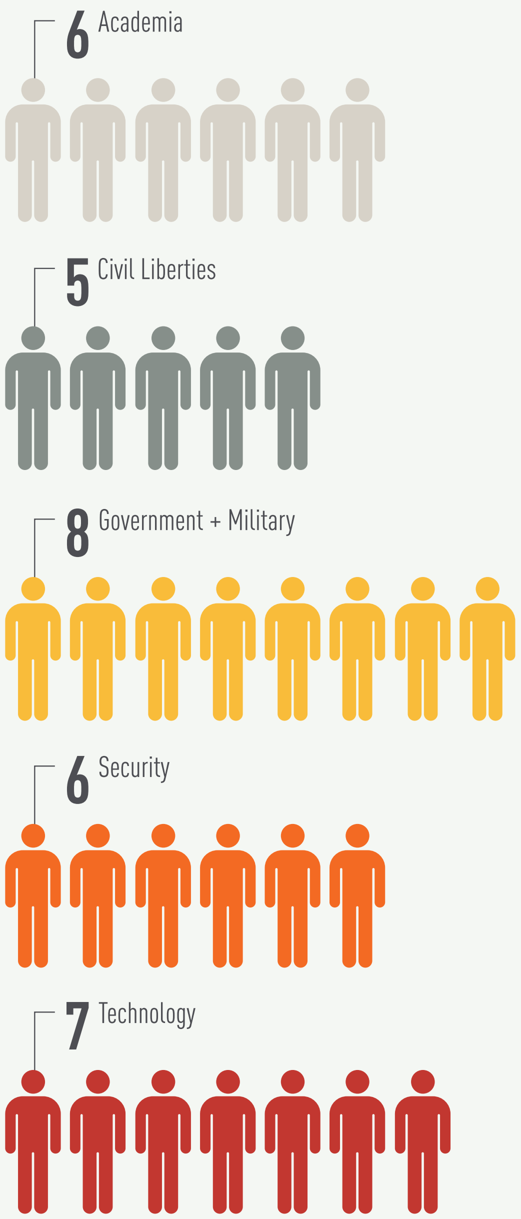
Who participated in the Delphi?

The Delphi included 32 leading cybersecurity experts from the US and abroad (see participant bios in Appendix D). We grouped participants into broad industry segments based on their background and affiliations. The segment labels are not intended to define our participants, and they also do not do justice to the wide-ranging diversity and interdisciplinary nature of our participants’ work. By grouping participants, we sought to analyze issues as popular across segments or contained within segments. The five segments are:

- Academia
- Civil Liberties
- Government and Military
- Security
- Technology

Again, we wish to thank our 32 experts for their participation in this unique project, and for their continued engagement throughout this multistage study.

Experts by industry segment

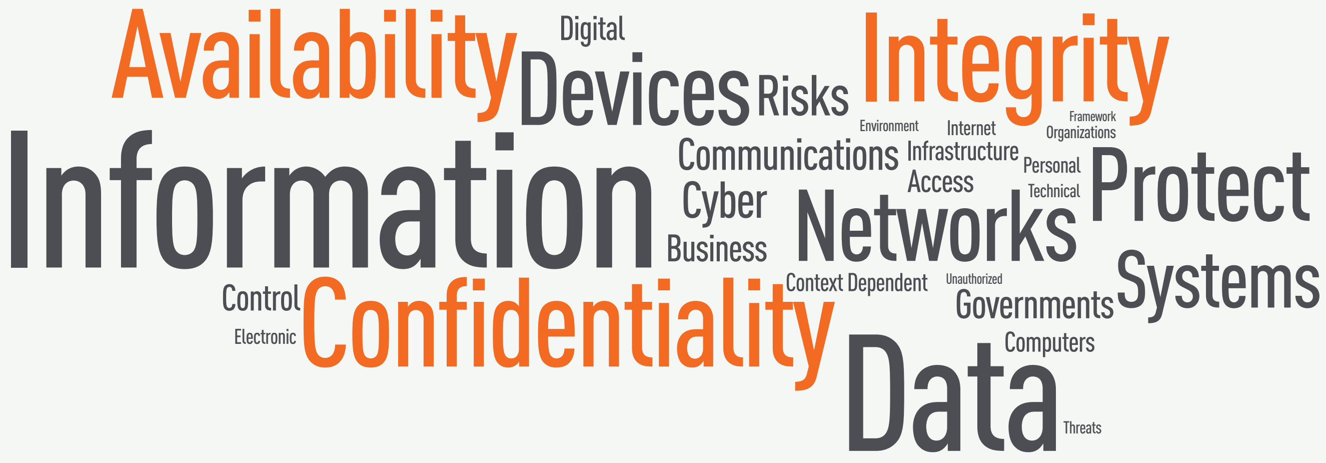


Agreeing on terms: defining cybersecurity

"Cybersecurity is freedom from fear of attack - unauthorized access or use of one's identity, data, network or system - by anyone, for any reason, in any way."

Key insights

- Our experts agree that cybersecurity is a broad and contested notion.
- Thus, most of them refer to an essential core of confidentiality, integrity, and availability of information as the key technical components of the cybersecurity definition.
- Context matters in defining cybersecurity: the definition should encompass nuances across scale, devices, actors, and types of risk.
- Framing also matters and should be included in the very definition of cybersecurity. Elements of human rights (notably privacy) and economics belong at the core of the notion.



The graphic above displays the key words used by experts in defining cybersecurity. The larger the word, the more often that word was mentioned in the definition.

Step one in a good policy conversation is agreeing on the goals and terms of the debate. More often than not, cybersecurity yields a lot of talking past each other, to the extent that some wonder if cybersecurity isn’t a Humpty Dumpty word:

> “When I use a word,’ Humpty Dumpty said, in a rather scornful tone, ‘it means just what I choose it to mean — neither more nor less.” -Lewis Carroll, Alice Through the Looking Glass

The common discourse around cybersecurity may often be confused and may stretch definitions to encompass a wide range of cyber incidents from crimes, to negligence, to wars and data breaches. But our participants, despite their varied backgrounds and perspectives, achieved significant consensus on how to conceptualize cybersecurity. Specifically, our experts viewed confidentiality, integrity, and availability of information as the key technical components of cybersecurity. Fourteen of twenty-nine respondents mentioned these three elements when we asked them to “define cybersecurity in [their] own words, including what, specifically, cybersecurity is trying to secure.”

Our experts did not feel the definition should stop there, however, insisting instead that the definition should include context. For instance, our experts referred to concepts such as multiple devices (i.e., Internet of Things) or fundamental rights (e.g., privacy) to be key components in a comprehensive definition of cybersecurity. Finally, participants often noted that securing people was ultimately the objective of cybersecurity.

> “[In defining cybersecurity], the focus on technology and data is widely known and appealing, but ultimately the people aspects are most important.”

> “Cybersecurity includes protecting against device manufacturers who surreptitiously act against the wishes and interests of the device owner or user. A device with a hidden backdoor is insecure.”

> “Cybersecurity is trying to secure both access to data (privacy/confidentiality) and computer operations (i.e. against attacks that would change or stop those operations). I’d say the first category is more about the readability of the data, while writeability of the data falls more under the second category.”

Our experts also highlighted that ‘cybersecurity’ was inherently a contested and broad notion and therefore subject to political instrumentalization. Some contrasted it with computer security, with, for example, a participant within the security segment explaining that the latter was “by itself more often concerned with tactics and the daily fight. Cybersecurity, on the other hand, is most often concerned with adjusting the environment and the underlying non-technical rules of the game in a manner in which actually changes the strategic, long term relationship between sides.”

Some participants suggested the difference between such terms was mostly political, with one expert arguing that cybersecurity and computer security were mostly synonyms, though cybersecurity was used “in government and military circles, including contractor and lobbyist circles” to connote that these questions were indeed a “tool and preoccupation of government.” This participant added: “it is worth noting that there are fundamentally different concerns and moral intuitions underlying different conceptions of security, including whose responsibility it is and whose interest it is meant to serve.”[1]

Finally, security of users should be viewed as the central focus of cybersecurity as noted by one expert in security: “cybersecurity secures not any one system but the ability to conduct business and continue operations in a routinely threatening electronic environment”. In that regard, one participant in civil liberties offered that cybersecurity needed to be thought primarily as any other form of human security: “When we talk about security for an individual or an organization, at the root, we are trying to defend the ability of that body to have the freedom, time and resources to achieve what it is they are meant to be doing, be that living daily life or accomplishing an important mission, without the interference of others.”

[1] This panelist referenced an academic paper on the topic: Nissenbaum, Helen. “Where Computer Security Meets National Security1.” Ethics and Information Technology 7.2 (2005): 61-73.

Users, tech & norms:

A broad picture of issues & levers in cybersecurity

Throughout rounds of our study, participants addressed a rich and diverse set of issues, demonstrating the many levers and priorities in the field of cybersecurity policy. When asked to focus on cybersecurity issues that should be a priority in the policy debate, they identified three solution vectors for a more secure digital world: the user environment, the technological environment, and finally the normative environment.

The user environment

Key insights

- People might be the problem, but blaming them isn't the solution: our experts think there is much to be done to help the average person make the right security choices.
- Automating the patching of critical security updates arose often as a desirable way to achieve this goal.
- Generally, anything to encourage secure by default technology is going in the right direction, although there is room for debate on what secure tech by default encompasses.

> "The more you can take people out of the process, the better."

Delphi participants agreed that there is much to be done to make it easier for people to make better choices in their everyday computer practices. For instance, in the case of cryptography, four times as many experts expressed a desire to make tools easier or automatic for the average person, as opposed to solutions oriented towards more education on cryptography or teaching people how to use encryption tools.[2]

Automation of security software updates in a manner that respects user autonomy was a popular and often discussed idea throughout the study was. A participant summarized the general tone of this conversation: "Patching of vulnerable software is probably the place to get the most immediate bang for the buck." Others looked for historical comparisons:

"[Perhaps we should consider] a degree of light-handed paternalism. For example, for major security updates, users should not necessarily bet presented by the option to install it, in the same way that children in the 1940s and the 1950s were required to get polio vaccines. We need to make it easier for users to make the right kinds of decisions."

When we asked which changes to individual uses of computer systems – i.e., those typically used by laypeople in homes, offices, and public places – would have the biggest positive impact on cybersecurity, 11 out of 32 respondents referred to automated patching. At least one person from each industry segment mentioned patching, but about half of the mentions came from the technology segment alone.

[2] Policy proposals to operationalize this idea included "Set up and fund open source task forces or working groups to make current security technology and services, notably cryptography, much easier to use for ordinary people" and "All things should be encrypted, push for greater use of cryptography."

“Take humans out of the loop as much as possible!”

It’s hard to operationalize this into specific policy solutions. When prompted for proposals they would like to see debated around the issue, our experts suggested:

- Convening a working group on what is acceptable in terms of automated patching of known bad systems and how to deploy such measures;
- Ensuring that firmware (notably in the Internet of Things and in routers) is easy to update through authenticated services;[3]
- Helping users make better decisions, notably vis-à-vis updates. For instance, “Do not ask ‘Do you wish to turn on automatic updates?’ but rather say, ‘If you are an ordinary user, you should click yes. It will ensure your system stays up to date with the latest security fixes.’”

Our experts often referred to the importance of education and user awareness, but also generally agreed that education could only go so far. One expert shared this perspective:

“Users are bad at security. This is no longer a hypothesis; it’s an absolute fact. We need to start building our security infrastructure around the idea that users have been and always will be our greatest security hole. We can’t rely on education to insulate them from attacks. We need to recognize that true systemic resilience needs to be able to exist in spite of users.”

Several experts insisted on solutions to make the environment easier to navigate for the user and to deploy secure-by-default choices. “Secure by default,” however, inspires different thoughts among our experts. Where one sees “home computers becoming image offerings that are kept clean and updated”, another describes “computer systems shipped from the manufacturer with the security settings fully enabled to automatically detect unauthorized devices, unauthorized software, unauthorized access.”

More thinking is needed about how to achieve wider deployment of solutions in this area. Most of the suggested actions revolved around supporting civil society and industry efforts that are already in motion in this area.

[3] An additional source for inspiration was suggested by one of our experts here: http://www.nsf.gov/cise/news/CybersecurityIdeasLab_July2014.pdf

The technological environment

Key insights

- Cryptography remains a priority: more needs to be done to deploy it widely and to make secure cryptographic tools easier to use.
- The public key infrastructure is a great source of concern: it should be "fixed asap!"
- Authentication stands as another hard problem to solve: policy should assist efforts to develop and deploy secure alternatives to passwords.
- Providing funding to sustain and supplement security efforts in free and open source software stands out as an obvious place to start.

Among the many technological issues cybersecurity policy should focus on, three stood out as tough challenges, calling for concerted efforts from all stakeholders: the wide deployment of cryptography, the security of the public key infrastructure, and the implementation of secure authentication mechanisms.

First, our experts have addressed the critical role played by cryptography in securing users, their computing and their communications. In that regard, cryptographic tools should be deployed more widely into existing systems, and tools to be used directly by people should be made much more accessible. Some frustration is apparent with recurring policy debates on cryptography, as much has been said on the policy trade-offs of cryptographic tools for law enforcement, but little progress is made to strengthen the state and deployment of cryptography.

Making the public key infrastructure secure and ensuring the trustworthiness of certificate authorities ("CAs") was also often noted by experts as both a tough problem to solve and a key priority for cybersecurity policy to take into consideration.[4]

[4] Proposals targeted at this issue included "Improve the PKI infrastructure, ensure browsers do not rely on CA controlled untrusted parties."

> "We need to make email encryption ubiquitous, and built into existing systems to make it as easy to use as secure HTTPS servers, i.e. fully transparent to the user. Securing web-based email is tricky but I'd like to see investments into inventing technology and email standards (via IETF) that could do it."

Developing better identity management systems than passwords was another popular discussion topic that consistently ranked as a priority for better cybersecurity, especially for changes to individual use of computer systems. Three quarters of our experts ranked this challenge among their top three priorities, and nearly one third as their number one priority for cybersecurity policy. Specific suggestions in this area included:

- Funding work and research to deploy alternatives to password;
- Encouraging better authentication technologies (not subject to gatekeeper's attacks) and examining incentives for wide adoption;
- Focusing on moving beyond default password configuration in the current CMS environment; and
- Providing some liability protection for companies using two factor authentication.

Participants saw the funding of security audits of critical open source projects as a key unresolved and priority issue in cybersecurity policy. Indeed, funding for free and critical open source projects emerged as an interesting outlier in becoming the one issue perceived by all as both highly desirable and feasible in a government cybersecurity policy agenda.

We believe the Heartbleed OpenSSL crisis may have contributed to this result, which demonstrates the desire for government involvement in cybersecurity policy in this area.[5]

[5] For specific actions targeted at this issue, see for instance the Linux Core Infrastructure Initiative.

The normative environment

Key insights

- Building norms for acceptable behavior in cyberspace was a popular priority for government action in cybersecurity across all segments of our expert group.
- Such norms should apply to governments, as well as to other stakeholders; corporations should also be concerned and involved in these efforts.
- Human rights should guide the building of such norms, and norms should be communicated and shared clearly and openly in the international arena.

The building of better norms regarding behavior in cyberspace is sometimes portrayed as a primarily governmental concern - we saw quite the opposite with the study, as the proposition was popular and prioritized across all segments of our panel.

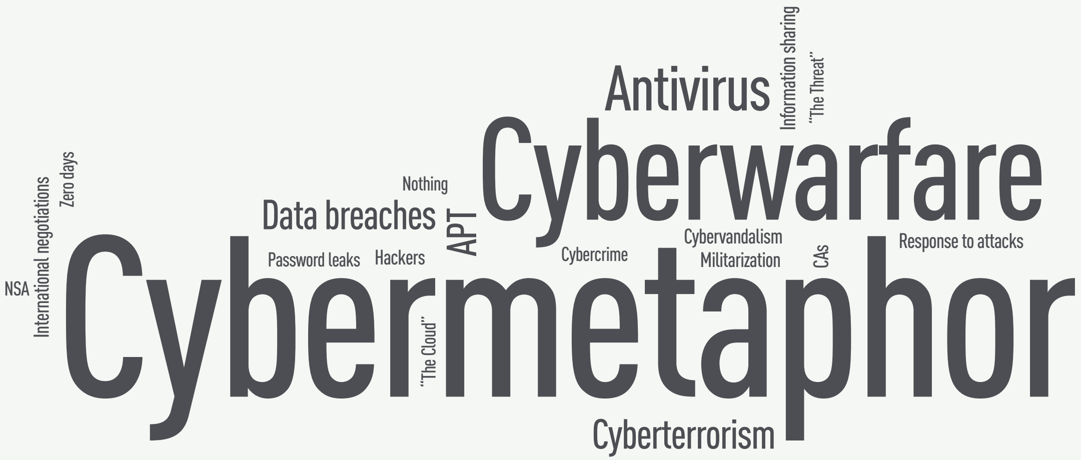
Norms had a slight edge over protection of trusted infrastructure by our experts as a priority issue for government involvement, and rated much higher in priority for policy action than enforcement of cybercrime, funding free and open software, notification of data breaches, incentives to the private sector, and public education.

The normative environment is about the broadest label that could be applied to cybersecurity policy. To quickly summarize what we've learned, we could divide it into norms for everyday interactions in cyberspace, norms and expectations when cyber incidents occur, and international norms to prevent conflict escalation in cyberspace. Needless to say, these propositions do not span the universe of normative issues and topics in cyberspace; they simply reflect the ones that made it to the final stage of our study.

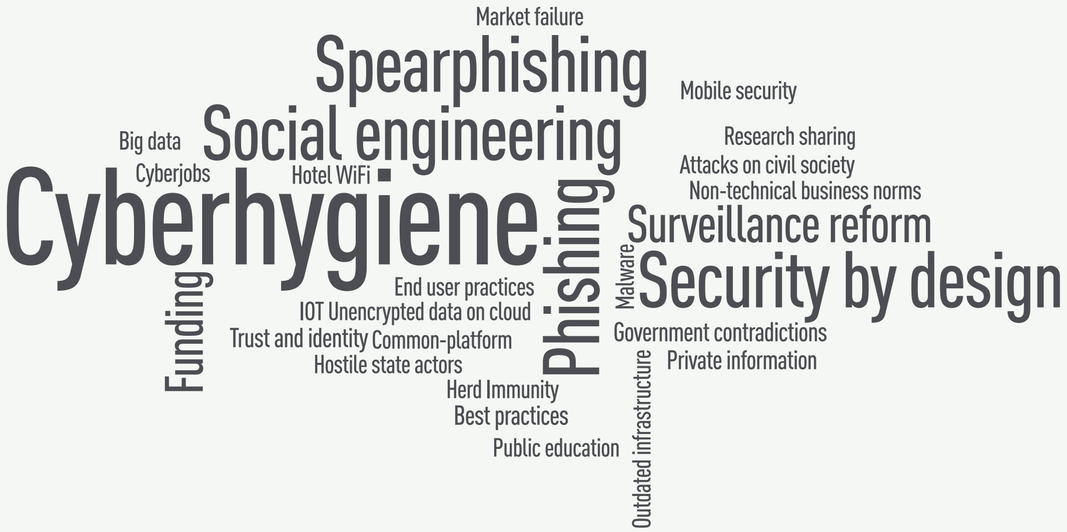
Regarding norms for everyday interactions in cyberspace, propositions included:

- Enacting better privacy laws;
- Changing the legal frameworks likely to provide a chilling effect for security and academic researchers ensuring that security researchers and entrepreneurs can tackle such questions without legal uncertainty;
- Allocating more resources to fight petty cybercrime; and
- Requiring notification to customers when their personal information is compromised.

Cybersecurity issues getting too much attention in the public debate



Cybersecurity issues not getting enough attention in the public debate



For the management of cyber-incidents once they have occurred, we engaged our experts in a pseudonymous discussion analyzing the role of government through the example of the Sony hack. A lack of clarity over who in government was in charge of addressing such incidents was duly noted, with one participant suggesting a RACI chart for government involvement in cyber-incidents would be a good exercise to undertake. Cyber-hyping here too was pointed at as an unhelpful reaction:

"After report of criminal activity, the government's role is to investigate, to secure the persons reasonably believed to have committed the offenses by arrest or extradition, to prosecute them, and to administer such penal sentences as the courts shall impose. When persons committing criminal offenses are agents or employees of foreign governments, the processes may be less certain in their effect, but the responsibility of the domestic government for law enforcement is neither reduced nor enlarged. Nothing about the events occurring with respect to Sony changes any of those obvious points in any way. The effort to find something different in this situation is just cyber-hyping, and should be resisted to the point of intentional efforts at abatement."

Our experts were very keen on discussing international norms. They felt that creating and communicating clear norms outlining acceptable behaviors in cyberspace while resisting the inflated cyber metaphors and taking human rights into strong consideration was a key priority for cybersecurity policy.[6]

The two word clouds above reflect what our experts feel gets too much attention in the public debate about cybersecurity (on the left), and what they feel does not get enough attention in the public debate (on the right).[7]

[6] Policy proposals related to this included "Clearer norms, including taking human rights into consideration, to bound States' activities in cyberspace" and "Publicly discuss and establish clear rules of the road on sensitive topics of government behaviors in cyberspace, and act in accordance with such rules."

[7] Exact questions to our experts were: "In the public debate, what 'cybersecurity topic' gets too much space and attention?" and "In the public debate, what 'cybersecurity topic' does not get enough space and attention?"

Cryptography, information sharing, and the protection of critical infrastructure

The elephants of cybersecurity policy

Key insights

- Participants with very different backgrounds identified cryptography, information sharing, and protection of critical infrastructure as high-priority cybersecurity policy targets.
- Cryptography runs through many different policy recommendations, as well as standing on its own as a priority, with participants citing the value of more usable and more ubiquitous cryptography technologies.
- Although information sharing is widely recognized as a policy target, some participants noted that the plethora of current mechanisms for information sharing has not converged into a fully functional framework.
- Protecting critical infrastructure is cited explicitly by many participants as a high priority target, as well as a natural role for government involvement.

Cybersecurity conversations are often dominated by three specific topics: cryptography, information sharing, and critical infrastructure. These are the issues we call the "elephants" in the room of cybersecurity. They are at the center of many policy dialogues - whether explicitly articulated or left silent, and they occupied a major place in our survey responses as well.

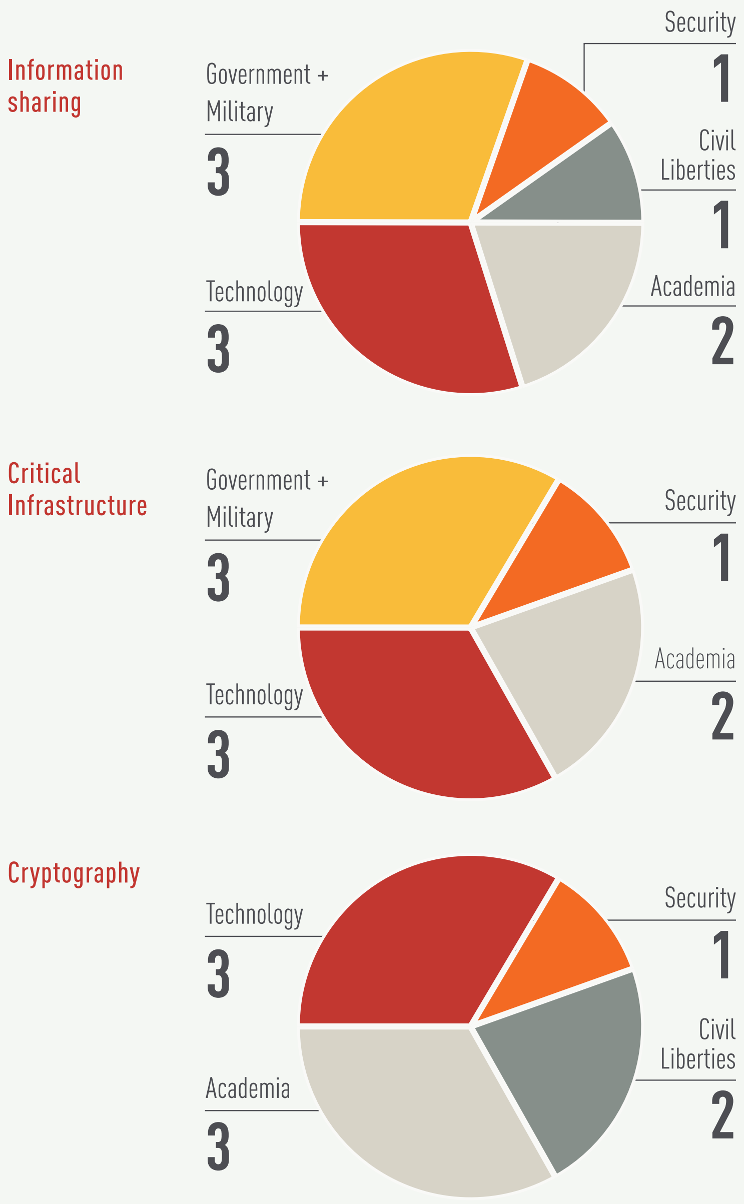
All three are fundamental to building security in the digital world, but, they must not be allowed to obfuscate the rest of the landscape. This section of our report brings the "cyberelephants" out into the middle of the room, so they can be isolated and analyzed on their own, and better separated from issues less developed and identified.

Cybersecurity is a complex landscape, and it's challenging to keep all of the pieces in mind at once. It's natural for a few to rise above others. The concepts that are important to the largest number of people, that have the longest and most well developed policy landscapes, and that are discussed the most often in media will dominate conversations because it's much easier to focus on one or a few things than many, as it is the case with these three specific issues.

From a segments perspective, cryptography is evenly noted by experts across all segments except from Government/Military, while information sharing and critical infrastructure are slightly more desirable among Technology and Government/Military.

These three "cyberelephants" emerged from our study as three of the most substantively important and frequently mentioned policy topics in cybersecurity. Without question, solving the myriad of problems inhabiting the cybersecurity landscape requires attention to improving the efficacy and ubiquity of cryptography; the design, baselines, and functionality of information sharing; and ample attention to the specific protection of critical infrastructure.

Top desirability ranking by segment for “Cyberelephants”



> “Until we get the basics right, information sharing as a practice domain will be wildly more costly than its benefits will warrant. In the future, mature high functioning organizations that are able to understand themselves, where they are, and what their real risks are ... will get a lot out of information sharing. At present, the list of those organizations is very short.”

Fortunately, these are all areas of active policy discussion and resource investment today. Legislation in the U.S. regarding information sharing is often controversial, but it has been in development for many years; in the meantime, private sector efforts have developed and promulgated. Websites of all stripes are moving to encrypted transport, just as user choices for secure communications abound more than ever before. Protection of critical infrastructure likewise remains at the top of the priority lists of many policymakers.

Yet, these “cyberelephants” often trample on other deserving cybersecurity policy priorities, or loom so large that it’s hard to see the other things that must be done to secure users and Internet infrastructure more broadly. The Mozilla Cybersecurity Delphi Project yielded 36 policy suggestions, only handful of which touch on these cyberelephants.

As policymakers shift to a more holistic, comprehensive understanding of the problems and solutions of cybersecurity, we hope they will not only engage with these “cyberelephant” issues, but also explore the many other areas that our experts identified as priorities in need of further investment.

A way forward:

towards a user-centric & holistic approach to cybersecurity policy

Throughout the four rounds of surveys and discussions of our Delphi project, there were no lack of problems and concerns for our experts to identify and diagnose. Poor cyber hygiene in government, misguided user behaviour, unacknowledged attack vectors, unreliable and widely deployed technology, all came up in due course. No shortage of issues, yet no clear path ahead: the cataloguing and evaluating of concrete cyber policy measures to increase user security in this context appeared to be a harder task than identifying what needed fixing.

It seems as if with cybersecurity challenges multiplying and growing increasingly public and complex, the policy debate in this area is not fully engaging with the diversity of challenges. We designed the Delphi project in hopes that it could help complete the cybersecurity policy picture and to assist with the overdue update the field needs. Cybersecurity policy has long been dominated by recurring conversations, including conversations held in similar terms about policy trade-offs litigated more than twenty years ago, as some have noted about the case of law enforcement and cryptographic backdoors. We would like this project to help guide policy makers towards a more holistic, comprehensive understanding of the problems and solutions of cybersecurity.

The three issues that grouped together in our findings, those we called the three "cyberelephants," represent the well charted grounds of cybersecurity policy and perhaps the longest running governmental conversations on cybersecurity. Privacy-respecting information sharing policies, efficient critical infrastructure protection, widespread and secure encryption: these are key objectives for cybersecurity, hard goals to achieve and issues on which the policy contours have been largely identified and abundantly debated. They represent both fundamental topics for cybersecurity policy and the issues that are most likely to obfuscate the rest of the levers, problems and parameters in the cybersecurity landscape.

Our process recognized the significance of these issues, but drawing on experts from a range of sectors and backgrounds, helped us dig deeper and produce a more nuanced and fulsome understanding of the cybersecurity problem and policy landscape. Differences in priorities, language and framing do appear between the segments (civil liberties, academia, technology, security and government & military) - as do common understandings across the segments, for instance with regard to the definition of cybersecurity and consensus for actions to prioritise, and in the case of security funding for free and open source software. This approach thus illuminates issues that appear as more consensual, desirable, or urgent than usually portrayed, as with the clear call for clear norms guiding stakeholder's behaviour in cyberspace, the need to prioritise solutions to increase the security of the public key infrastructure, and the need for policies encouraging better authentication mechanisms.

A user-centric cyber security policy agenda is one that provides people with, as one participant said, "freedom from fear of attack, unauthorised access or use of one's identify, data, network or system - by anyone, for any reason, in any way." It is a set of solutions that increases our global security without putting the burden on the user, by identifying solutions and levers that build a more secure world for all. We believe our Delphi project articulates and defines road markers on the way forward to such an agenda.

Appendix A: Policy list

The Mozilla Cybersecurity Delphi Project began very broadly, asking 17 open-ended questions. After multiple steps of priority setting and discussions, our expert panel produced a long and wide list of cybersecurity policy suggestions and possible areas where government can play a role.

As stated earlier in this report, the suggestions and possible solutions in itself is not the intended core focus, but rather the insights and transparent process involving a variety of industries and the willingness of a panel of experts to engage in a dialogue over this complex issue.

The following 36 cybersecurity policy suggestions, in no particular order, come from a balanced mix of experts across industry segments:

1 Better privacy laws.

2 Require notification to the customers when their personal information is compromised.

3 Better protect critical infrastructure, define sufficient security measures and audit critical sectors to ensure / enforce that relevant private sector actors meet the requirements.

4 Provide some liability protection for companies using two-factor authentication.

5 Change the legal frameworks that provide a chilling effect for security researchers and academics, ensure that security researchers and entrepreneurs can tackle such questions without legal uncertainty.

6 Make all Government software free software and auditable, which would allow for more security in both the governmental and the non-governmental users.

7 Create a safe (legal) environment for actors to share information with the public and the industry after cyber attacks.

8 Clearer norms, including taking human rights into consideration to bound States' and companies' activities in cyberspace.

9 Publish official guidelines and provide reference implementations addressing how can government bureaucracies and corporations better defend themselves.

10 Publish a clear international strategy to increase risks and consequences for adversaries attacking through cyberspace.

11 Develop a consensus framework to survey all the various problems that exist in the cybersecurity space.

12 Work to research and deploy alternatives to password, encourage authentication technologies that are subject to gatekeeper attacks, examine incentives for wide adoption. Help move beyond default password configurations in the current CMS environment.

13 Convene a working group on what is acceptable in terms of automated patching of known bad systems and how to deploy such measures.

14 Encourage better code-writing practices, design due diligence processes for security checks of written code and product assembly.

15 Have government agencies set up task forces or working groups to help organizations think through better systems for vulnerability management across their organizations.

16 More research on cybersecurity vulnerabilities in engineering complex systems.

17 Encourage Government and NGO to create labels / seals of approval for corporations and government services meeting certain security standards.

18 Encourage greater inter-governmental coordination on cyber response (e.g. between state and federal levels in U.S.).

19 Ensure the intelligence community does not corrupt secure data standards.

20 Publicly discuss and establish clear rules of the road on sensitive topics of government behaviors in cyberspace, and act in accordance with such rules.

21 Encourage and support intra-governmental collaboration, partnerships and other trust building work to combat fracturing of efforts along national defense lines

22 Ensure firmware (notably in IoT, routers, etc.) is easy to update through authenticated service.

23 Develop federated compatible identity systems that are widespread and do not rely on government-issued key.

24 Re-think basic Internet protocols from the ground up to build security at the core.

25 Improve the PKI infrastructure, ensure browsers do not rely on CA controlled by bad governments.

26 Help user make better decisions, notably vis à vis the updates. Do not ask, "Do you wish to turn on automatic updates?" but precise "If you are an ordinary user, you should click yes. It will ensure your system stays up to date with the latest security fixes."

27 All things should be encrypted, push for greater use of cryptography.

28 More resources need to be allocated to fighting petty cybercrime, not just IP theft by other nations through cyber means.

29 More funding for development and maintenance of secure open source / free software tools, with a priority on critical and widely deployed projects.

30 Allocate more funds to independent research and development actors providing easy-to-use tools for cybersecurity and working on user awareness and education.

31 After each data breach, work on what are the best practices and procedures that could help prevent this in the future. Provide "This is what you should have done / this is what went wrong / this is what you should always do first / this is what you need to do every day" type of guidelines.

32 Widely deploy cybersecurity education in schools and in other aspects of Government programs.

33 Fund programs to educate users to use encryption and encrypted communications tools.

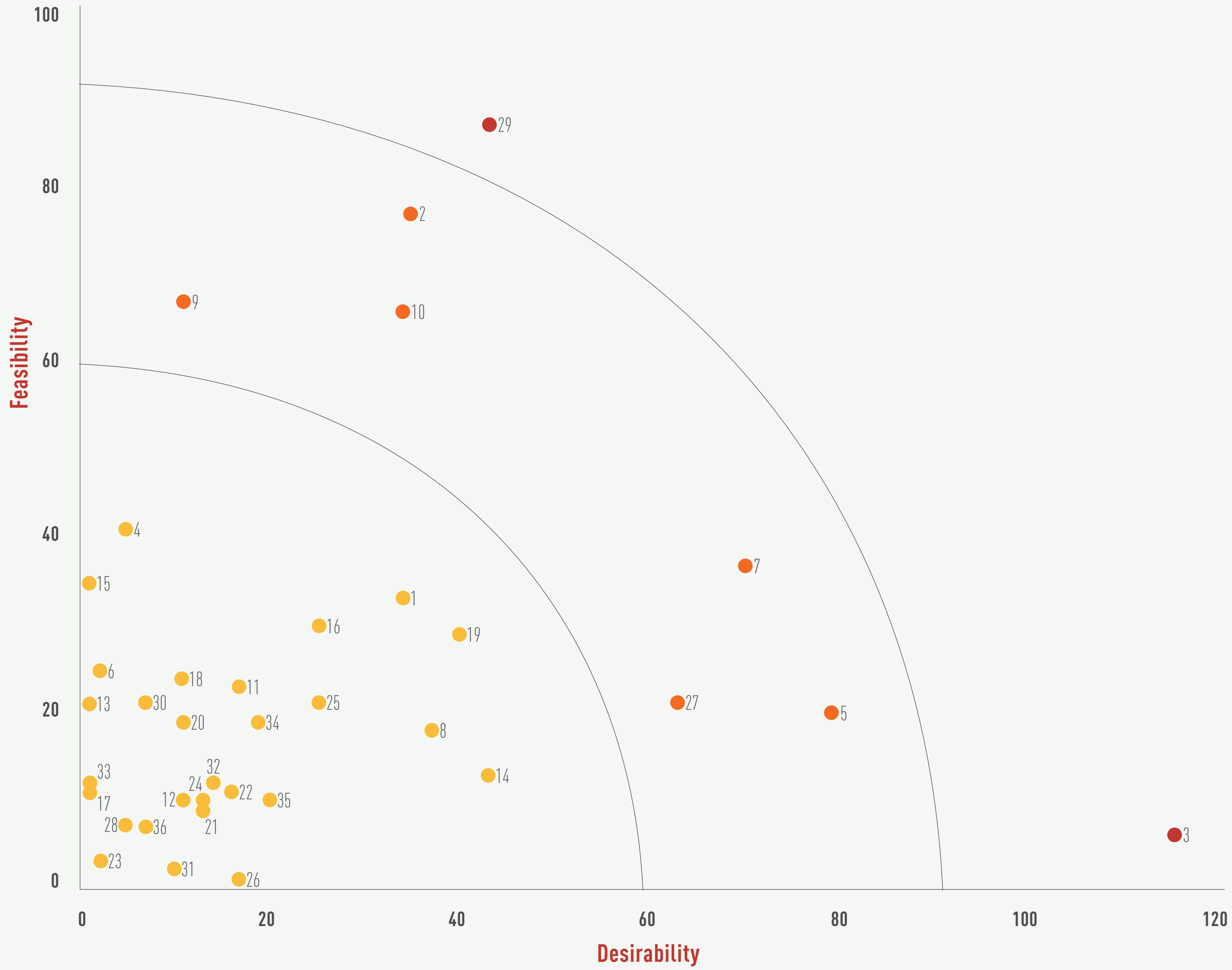
34 Structure a strong model to identify fundamental open source software resources and projects and fund proper security audits, allocating enough resources.

35 Set up and fund open source task force to make current security technology and services, including crypto, much easier to use for ordinary people.

36 Attract and adequately compensate people able to work within Government and with all parts of Government to ensure basic security is met throughout all services, ex. all .gov websites in HTTPS-only.

Appendix B: Weighted scatterplot of all suggestion

Weighted scatterplot of 36 policy suggestions



The final step of the Delphi asked the panel of experts to rank their Top 5 Desirable and Top 5 Feasible issues from the full list of cybersecurity policy suggestions. A total of 27 experts engaged in this exercise, and while sample sizes may be small for any particular policy, some themes emerged in what our experts found desirable and feasible. The scatterplot applied a weighted score for both desirability and feasibility, thus Rank 1 was given the highest score and Rank 5 the lowest score.

Weighted score:

rank	pts
1	16
2	8
3	4
4	2
5	1

Numbers in the scatterplot correspond with the specific policy suggestions in Appendix A.

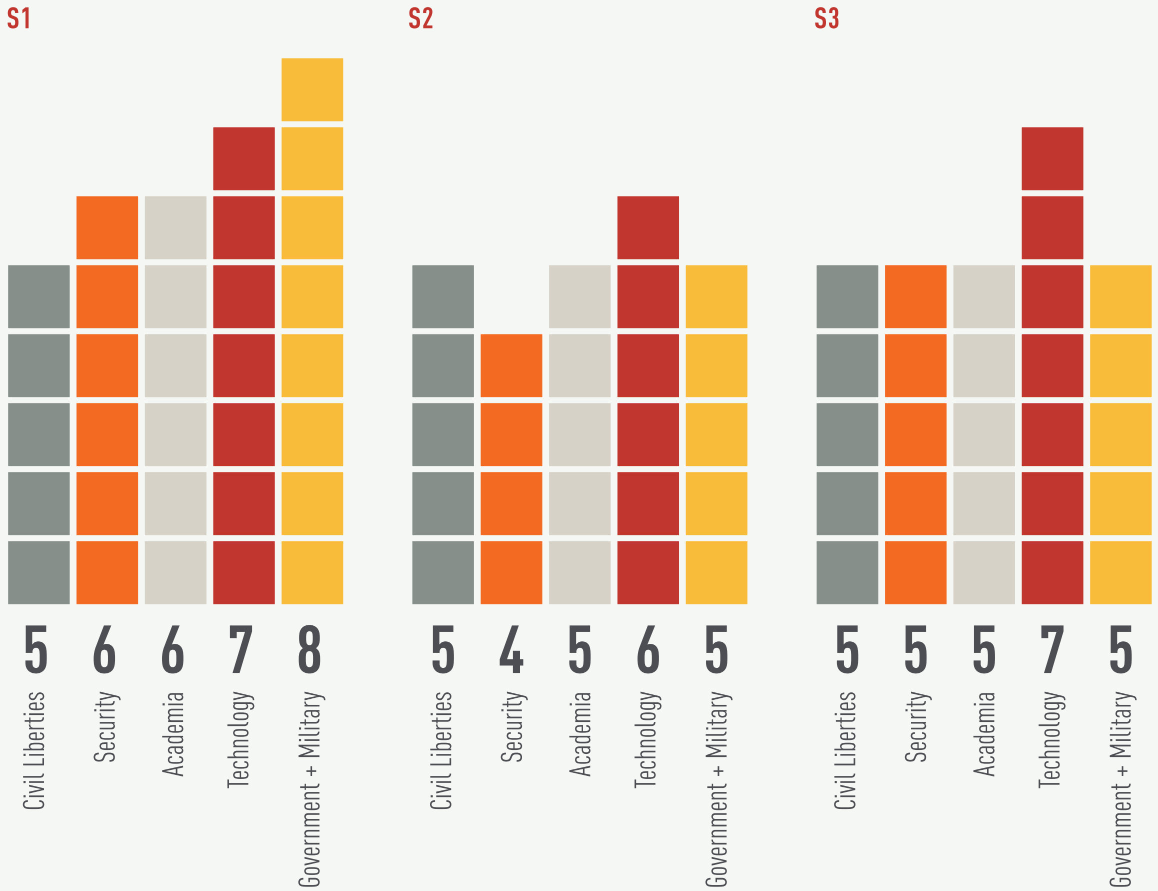
As a cautionary note, findings are not meant to be statistically generalizable to the general population of cybersecurity experts.

Appendix C: Participant engagement

The Mozilla Cybersecurity Delphi Study began with more than thirty leading experts in cybersecurity, and a significant majority stayed engaged throughout each step of the study. Below are some considerations of the Delphi Project, followed by a graph showing segment engagement in each major study phase:

- The first phase of the Delphi (S1) involved the greatest number of participants (32), and contained the largest and widest range of responses.
- Several participants from each industry segment did not participate in subsequent phases (S2 and S3), however, the segments remained evenly distributed as no one group saw large drop-off in any one phase.
- The panel's segments (academia, civil liberties, government & military, security, and technology) were fairly even in size at the start and end of the study, thus giving equal weight across segments.

Delphi engagement by segment



Note: The Delphi technique is often time consuming and it is not uncommon to see drop off in participation during the various stages of research.

Appendix D: Participant bios

Kevin Babcock is Principal Security Engineer at PagerDuty, the leader in operations performance management. He has over 15 years of experience in the information security field, including application security, authentication, encryption, Web security, anti-spam, and network security. He has worked with organizations such as Symantec, SafeWeb, and Box. Babcock holds a B.S. in Engineering and Applied Science from the California Institute of Technology, and is a Certified Information Systems Security Professional (CISSP).

Chris Camacho is the Security Vice President for Bank of America, responsible for malware response and the Bank's Cyber Event Response Team (CERT). He previously worked at The World Bank Group to develop security technology initiatives, and was responsible for cyber intelligence within the Group. Camacho is a respected researcher in the information security community and an active member of the FS-ISAC Threat Intelligence Committee.

Dr. Ron Deibert is Professor of Political Science and Director of the Citizen Lab at the University of Toronto's Munk School of Global Affairs. The Citizen Lab focuses on the intersections between the Internet, security and human rights. Professor Deibert has authored numerous publications on these topics, and has consulted governments and organizations on related issues. He was appointed to the Order of Ontario in 2013, and awarded the Queen Elizabeth II Diamond Jubilee medal for being "among the first to recognize and take measures to mitigate growing threats to communications rights, openness and security worldwide."

Andy Ellis is Akamai's Chief Security Officer, responsible for overseeing the security architecture and compliance of the company's massive, globally distributed network. He is the designer and patent holder of Akamai's SSL acceleration network, as well as several of the critical technologies underpinning the company's Kona Security Solutions. Andy is at the forefront of Internet policy; as a speaker, blogger, member of the FCC CSRIC, supporting Akamai's CEOs on the NIAC and NSTAC, and an advisory board member of HacKid. He is a graduate of MIT and a former US Air Force officer, the recipient of the CSO Magazine Compass Award, the Air Force Commendation Medal, The Wine Spectator's Award of Excellence, and the Spirit of Disneyland Award.

Marshall Erwin works for Mozilla as a senior staff analyst with a focus on data security, privacy and surveillance. Previously, he spent five years as a counterterrorism and cybersecurity analyst in the Intelligence Community. He also served as the counterterrorism advisor to Senator Susan Collins on the Senate Homeland Security and Government Affairs Committee and as the intelligence specialist at the Congressional Research Services. He was a fellow at Stanford University's Hoover Institution. Erwin holds an M.P.P. from Georgetown University, and a B.A. in philosophy and B.S. in computer science, both from Stanford University.

Adam Firestone is President and General Manager of KGSS, Inc., which provides cybersecurity intelligence, systems engineering services, and product solutions to government organizations. Firestone is also an Adjunct Professor at Georgetown University, a former United States Army Officer, and previously practiced law in the State of New York. He holds degrees from Yale University and Brooklyn Law School.

Dr. Matthew H. Fleming currently leads the cybersecurity resilience program of a large financial services firm in the United States. Having held positions with the U.S. Department of Defense, International Monetary Fund, and others, Fleming is also an adjunct professor at Georgetown University, with the McDonough School of Business and McCourt School of Public Policy. He is a nonresident fellow with New America and the GW Center for Cyber & Homeland Security, and an advisor to the Tech Council of Maryland and Washington Cyber Roundtable. He holds a Ph.D. in Public Policy from the University of London (University College London); a Master of Public Policy from the University of Michigan (Ann Arbor); and a B.A. in American Studies from Yale University.

Camille François served as the lead researcher for the Delphi project. Camille is a researcher, consultant and lecturer on cyber policy, with a focus on questions relating to cybersecurity, fundamental rights and state interactions in cyberspace. A Fellow at the Harvard Berkman Center for Internet and Society, Camille has also worked with organizations such as the U.S. Defense Advanced Research Projects Agency (DARPA), the French Prime Minister's Office, Google and the French-American Foundation.

She holds a Masters Degree in Human Rights from the French Institute of Political Sciences (Sciences-Po) and a Masters Degree in International Security from the School of International and Public Affairs at Columbia University.

Nathan Freitas leads the Guardian Project, an open-source mobile security software project, and directs technology strategy and training at the Tibet Action Institute. His work at the Berkman Center focuses on tracking the legality and prosecution risks for mobile security apps users worldwide.

Joseph Hall works as the Center for Democracy and Technology's Chief Technologist. He focuses on the intersection of law, technology, and policy and provides technical expertise to CDT's efforts to ensure that the internet remains free and innovative. Previously, Hall was a postdoctoral research fellow at New York University, Princeton University, and the University of California, Berkeley. He received his PhD from UC Berkeley in 2008, where his doctoral thesis examined electronic voting as a case study in digital government transparency. He also holds master's degrees in astrophysics and information systems. In 2012, the Election Verification Network honored Hall with the John Gideon Memorial Award for his work in the field.

Jonah Force Hill is an Adjunct Fellow with the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS). He works, writes, and speaks on a variety of national and international Internet and cybersecurity policy issues. He has served as teaching fellow for the course "International Cybersecurity: Public and Private Sector Challenges" at Harvard University; as an intern, consultant, and researcher in the Office of the Cybersecurity Coordinator at the National Security Council; and as a research assistant to General David H. Petraeus (USA, ret.). His writings have appeared in numerous publications, including Lawfare, the Atlantic, Harvard's National Security Law Journal, and the Georgetown University Journal of International Affairs. He holds an M.P.P. from the Harvard Kennedy School, an M.T.S. from Harvard Divinity School, and a B.A. from the University of California at Los Angeles.

Chris Ipsen is the State of Nevada's Chief Information Security Officer and Chairman of Nevada's State IT Security Committee. He previously served as Nevada's Chief Enterprise Architect, CISO, and Chief IT Manager, in which position he created an enterprise system that saved Nevada $2.5 million over four years. He was named the 2015 CSO of the Year by SC Magazine. Ipsen received a bachelor's degree in Public Administration from the University of Nevada, Reno.

Mischel Kwon is the President of security consulting firm MKA Cyber, which specializes in technical defensive security and information assurance. Kwon has close to 30 years of experience, and has served in many IT executive positions, such as Director of the United States Computer Emergency Readiness Team (US-CERT) and Deputy Director for IT Security Staff at the United States Department of Justice. She is an adjunct professor at George Washington University, and runs the institution's Cyber Defense Lab. Kwon holds a master's degree in computer science from Marymount University and a graduate certificate in Computer Security and Information Assurance.

Dr. James Andrew Lewis is a program director and senior fellow at the Center for Strategic and International Studies (CSIS). His recent work focuses on cybersecurity, international security, and innovation. He maintains a close research partnership with the China Institutes of Contemporary International Relations and advised the UN for the 2010, 2013 and 2015 negotiations on cybersecurity. Lewis' expertise is widely sought out by media outlets and leaders, with his report on "Cybersecurity for the 44th Presidency" receiving praise from President Obama. Lewis received his PhD from the University of Chicago.

Daniel Lohrmann has held numerous leadership positions related to cybersecurity and technology, including Chief Security Officer, Chief Technology Officer and Chief Information Security Officer for the State of Michigan. Lohrmann is currently the Chief Security Officer and Chief Strategist for Security Mentor, Inc., which provides online security awareness training. Lohrmann is a sought-after author, blogger, and keynote speaker. He has given presentations at events worldwide, and writes a regular cybersecurity column for Government Technology magazine. He holds a master's degree in computer science from Johns Hopkins University.

Shawn Lonergan is a Political Science PhD candidate at Columbia University and an active-duty major in the United States Army. He currently researches state interactions in cyberspace, cyber-ethics and security, and Internet governance. His past work includes a deployment to Iraq, work in cyber operations for the U.S. government, and studies at both Columbia University and the United States Military Academy at West Point, where he is now an instructor. Lonergan has been honored with numerous awards, including the Bronze Star and the Intelligence and Security Command MacArthur Leadership Award.

Jane Hall Lute is President and CEO of the Council on CyberSecurity Leadership and a member of the Department of Homeland Security Advisory Council. She previously served as the United States Deputy Secretary of Homeland Security, the United Nations Assistant

Secretary-General for Peacebuilding Support, and the Assistant Secretary-General for Mission Support in the United Nations' Department of Peacekeeping Operations. Lute holds a PhD in Political Science from Stanford University and a J.D. from Georgetown University.

James Marshall is the founder, President, and Technical Director of the Berkeley Institute for Free Speech Online and a leading expert on circumventing Web censorship. Marshall has been involved in the development of the Internet since 1990 and designed the popular open-source anti-censorship software CGIProxy. In the mid-1990s, he played a role in developing the infrastructure of the Web by working on Web-related technical standards (RFCs) and writing influential tutorials on HTTP and CGI. Today, Marshall works through BIFSO to maintain CGIProxy while also supporting other anti-censorship projects.

Danny McPherson is Senior Vice President and Chief Security Officer of Verisign, where he manages all aspects of the company's security. He has over 20 years of experience in the industry and has served on numerous task forces, boards and committees related to Internet operations and standardization. McPherson has authored several books, research papers, and numerous publications.

Eben Moglen is a Professor of Law and Legal History at Columbia University Law School where he has taught since 1987, and also serves as Director-Counsel and Chairman of the Software Freedom Law Center. He has represented many prominent free software developers, and was awarded the Electronic Frontier Foundation's Pioneer Award for his work toward freedom in electronic society. Professor Moglen received both his Law degree and a PhD in History from Yale University, and is admitted to practice in the State of New York and before the United States Supreme Court.

Mark Nottingham is the Chair of the IETF HTTP Working Group, and an elected member of the W3C Technical Architecture Group. He also serves as the liaison manager between the two organizations and works for Akamai, the world's largest public content delivery network. Nottingham has over fifteen years of experience in Web and technology development, and frequently makes substantial contributions to W3C Recommendations and IETF RFCs regarding web-related topics. He currently lives in Melbourne, Australia.

Brian Pascal is a nonresident fellow at Stanford Law School's Center for Internet and Society, where he focuses on the intersection of security, privacy and technology. His current research surrounds changes in power dynamics as a result of developing technologies. Pascal also has experience as a cybersecurity consultant with IBM, a civil liberties engineer with Palantir Technologies, and as an attorney. He completed his undergraduate studies in Physics at Duke University before studying science writing at the Massachusetts Institute of Technology and earning his law degree from the University of Michigan Law School.

Dr. Abel Sanchez currently conducts research and teaches at the Massachusetts Institute of Technology (MIT). He specializes in topics such as Big Data, Simulation, and Complex Systems. His research has included projects with companies like Walmart, Ford Motor Company, and IBM. Dr. Sanchez also teaches graduate level courses in Cyber Security, Data Science, and Software Construction/Architecture at MIT, and earned his PhD from the institution.

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by The Economist. He is the author of 12 books -- including the New York Times best-seller "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World." Schneier is a fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, and an Advisory Board member of the Electronic Privacy Information Center. He is also the Chief Technology Officer of Resilient Systems, Inc.

Seth Schoen has over 10 years of experience at the Electronic Frontier Foundation (EFF) helping technologists connect their work to civil liberties and legal initiatives. His work helps the public better understand technology-related products. He has been actively involved in digital copyright law and encryption since the 1990s, and has testified before the U.S. Sentencing Commission, the U.S. Copyright Office, and a variety of courts.

Amie Stepanovich is the U.S. Policy Manager for Access. Her areas of expertise include privacy law, domestic surveillance, and cybersecurity. Stepanovich has testified in hearings in both the Senate and the House of Representatives as the Director of the Domestic Surveillance Project at the Electronic Privacy Information Center, and was named a Privacy Ambassador by the Information and Privacy Commissioner of Ontario, Canada. In 2014, Stepanovich was recognized as one of Forbes magazine's 30 under 30 leaders in Law and Policy. She holds a J.D. from New York Law School and a B.S. from Florida State University.

Noah Swartz works with the Electronic Frontier Foundation (EFF), a leading nonprofit focused on civil liberties in the digital world. As a Staff Technologist on the Tech Projects team, he works on the software maintained and produced by EFF, such as Privacy Badger. Swartz has also worked as a researcher in the MIT Media Lab and as a free software/ culture advocate.

Dr. Motohiro Tsuchiya teaches at Keio University's Graduate School of Media and Governance in Japan. He has also taught at the International University of Japan, and was a visiting scholar at Massachusetts Institute of Technology, the University of Maryland, and other institutions. Professor Tsuchiya's work currently focuses on international relations, regulations and governance technologies. He has authored and co-authored many books and publications. Professor Tsuchiya earned a B.A. in political science, an M.A. in international relations, and a PhD in media and governance from Keio University.

Dan Veditz is the Platform Security Lead at Mozilla. He has previously worked as a Software Engineer for Netscape and Borland. He holds a B.S. in Physics and a B.A. in Classics from the University of California, Los Angeles.

Heather West works on the Public Policy team for Cloudflare, a cloud-based system designed to enhance website performance and "build a better web." Previously, she worked as a Federal Public Policy Analyst for Google with a focus on cybersecurity and digital privacy, and as a Policy Analyst for the Center for Democracy and Technology. West was recognized in 2014 as one of Forbes magazine's 30 under 30 in Law and Policy. She holds a B.S. in Computer Science and Cognitive Science from Wellesley College.

Jack Whitsitt is a principal Analyst for Energysec. A participant in the national critical infrastructure protection dialogue for seven years, Jack has provided regular advice, insight, and thought leadership to all levels of government and industry. His background has included facilitation, cutting-edge technical research & development, national control systems incident response, community building, large scale data analysis, Sector Specific Agency program development & execution, and more. Recently, Mr. Whitsitt was cited as an author in a NATO-sponsored report to develop Cybersecurity Confidence Building Measures intended to help nations avoid unintentional conflict escalation in cyberspace and has participated in formal "Cyber Norms" discussions about sources of instability in cyberspace, cyberwar, deterrence, and related topics.

Dr. Josephine Wolff will join the faculty of Rochester Institute of Technology in fall 2015 in the departments of public policy and computing security. She researches cybersecurity and Internet policy with an emphasis on understanding the interactions between different types of technical, social, and policy-based defensive mechanisms for computer systems. Wolff was recognized in 2011 as a Google Fellow for the Center for Democracy and Technology and is a fellow at Harvard University's Berkman Center for Internet and Society. She received a PhD in Engineering Systems and MS in Technology & Policy from MIT and holds an AB in mathematics from Princeton University.

Dale Wooden owns Weathered Security, a cybersecurity company which helps "regular citizens" protect themselves from cyberwarfare. Wooden has 20 years of active duty experience in the United States Navy. He has spoken at multiple conferences about cybersecurity, and has published works on the relationship between IT Security and corporate interests.

This report was authored by Camille François, Chris Riley, Jochai Ben-Avie, Dave Steer, and Su Midghall, and published in July 2015. This study was designed and conducted by Camille Francois & DHM Research.

This work was made possible by a generous grant from the **John D. and Catherine T. MacArthur Foundation.**

The MacArthur Foundation supports creative people and effective institutions committed to building a more just, verdant, and peaceful world. In addition to selecting the MacArthur Fellows, the Foundation works to defend human rights, advance global conservation and security, make cities better places, and understand how technology is affecting children and society. More information is at www.macfound.org.