REIMAGINING VISUALS FOR CYBERSECURITY

AUTHORED BY

openIDEO

CREATED FOR

WILLIAM + FLORA
Hewlett
Foundation

Written by

Hannah Lennett
and Scott Shigeoka

With support from

Heath Wickline,
Monica Ruiz, and
Eli Sugarman

Designed by

Erika Díaz Gomez

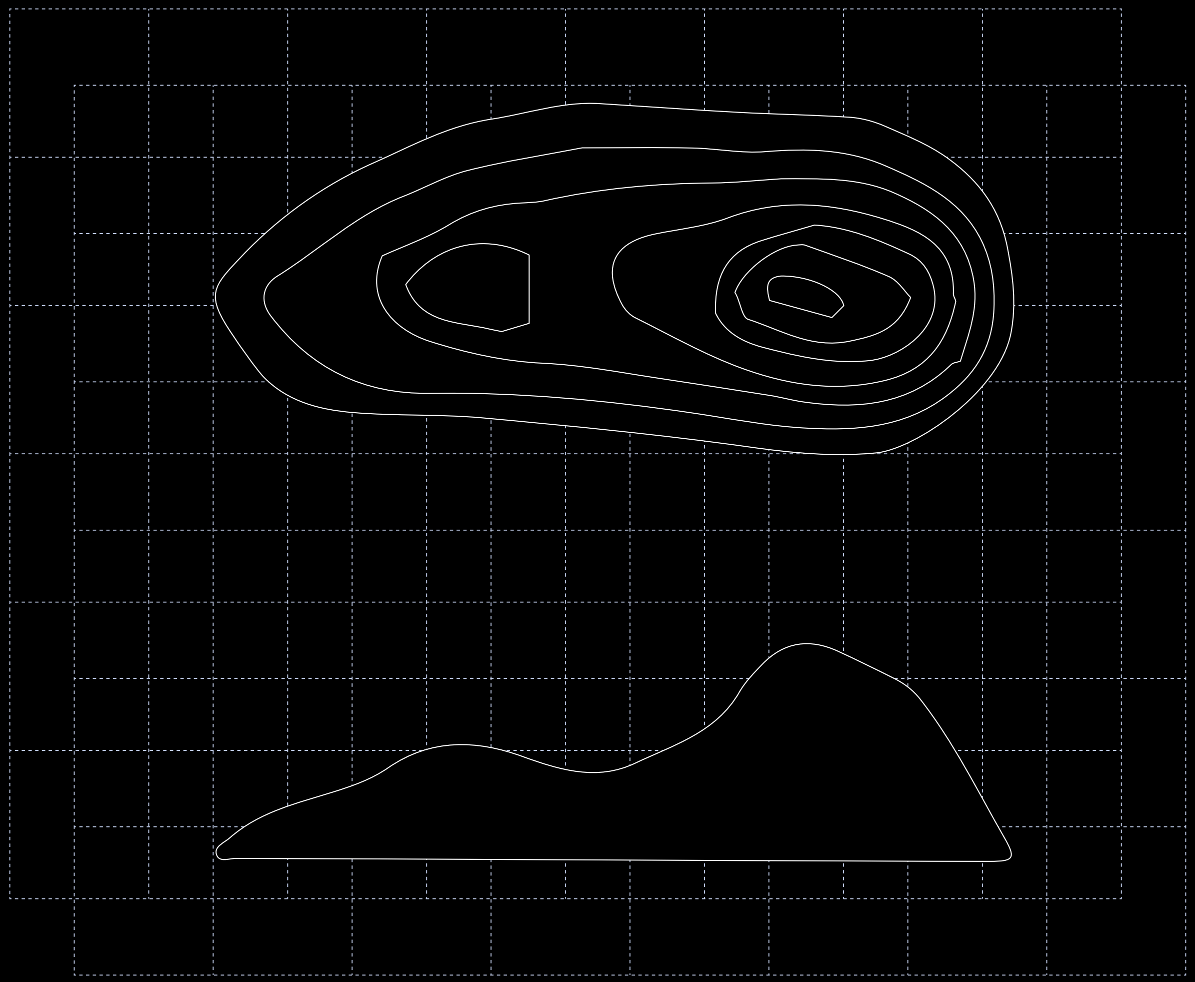
As you go through this report, there are some things we want you to know.

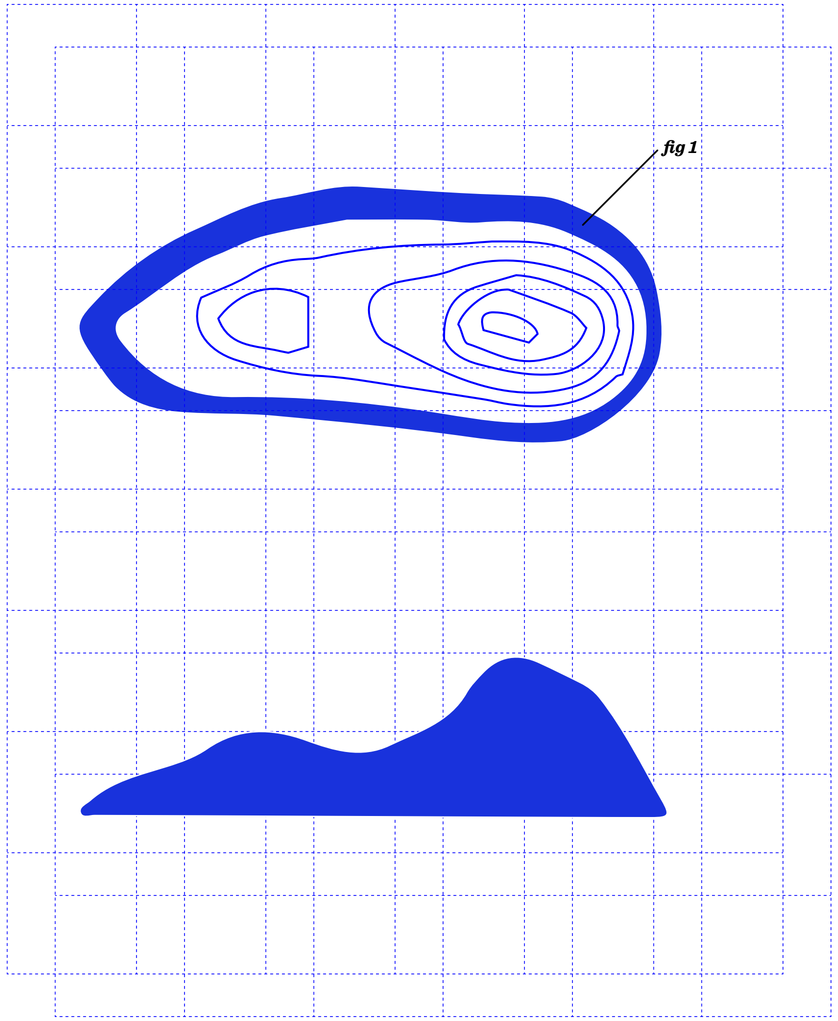
1 The process to create this report was an accelerated one, and not meant to represent every aspect of the field. This report is intended to give visual creators an introduction to the cybersecurity space to help you design better visuals for it. We hope it inspires you to do your own research and learn more about the topic.

2 This report itself—and the images within it—are meant to be provocations for possible visual directions, based on our research.

3 The color scheme of this report is black and white, with blue accents, to aid in connecting with the existing visual language of cybersecurity, while also bringing in new design elements to help introduce the possibility of new cybersecurity visuals.

CONTENTS





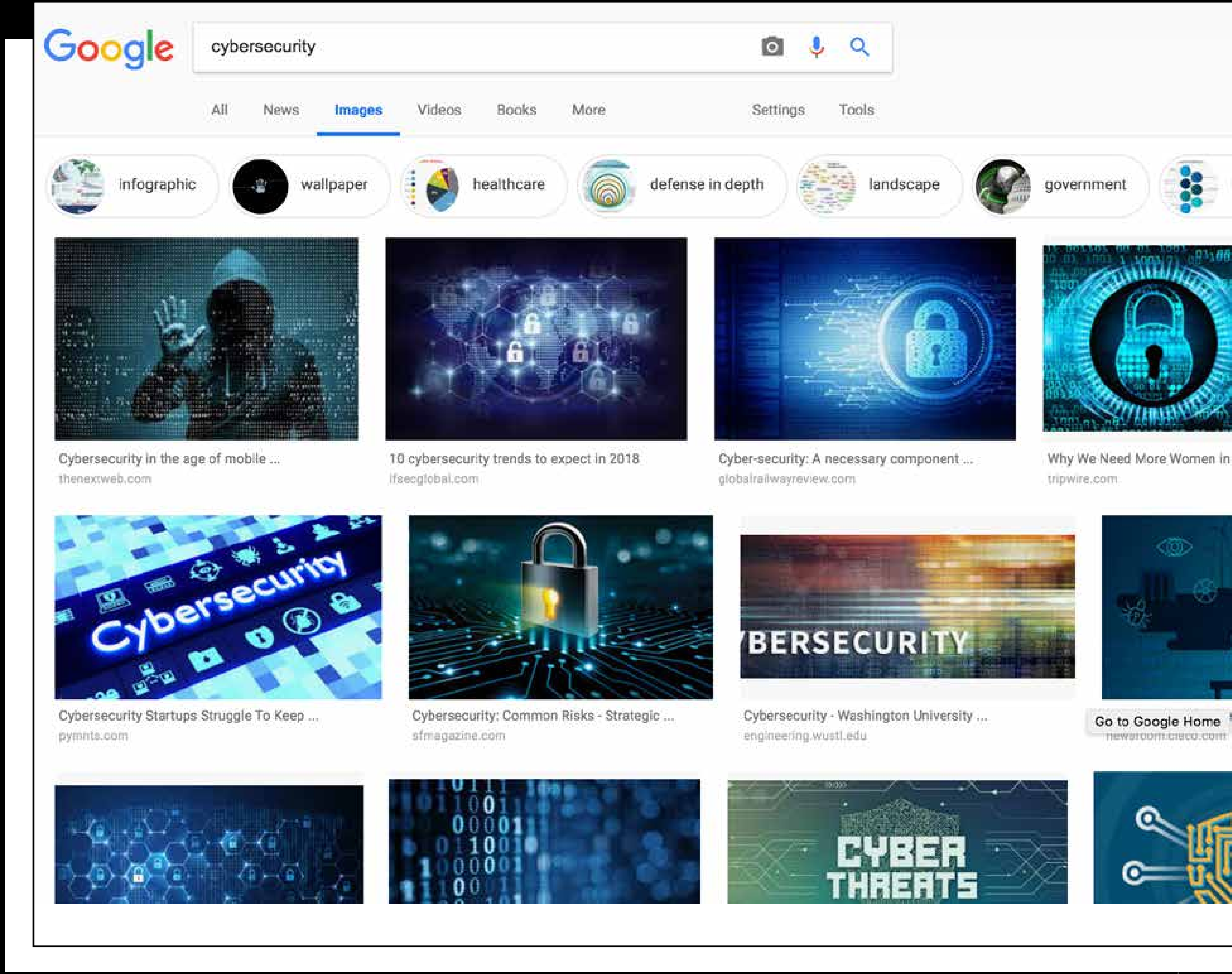
Chapter 1

CONTEXT

This report is intended for visual creators who hope to design for the cybersecurity space, offering background information about the field, and guiding questions and tools for future design work. We start by setting the stage and sharing how we conducted our research.

THE STATE OF VISUALS

When you do a Google image search for “cybersecurity,” you’ll find a repetitive stream of locks, green-lit code, server rooms, guys in hoodies hunched over glowing keyboards, or some combination of those elements. Policymakers, journalists, academics, and private sector and civil society experts all use them to illustrate their published work, despite almost unanimously agreeing that they do not accurately represent the field to which they have passionately dedicated their lives.



Google cybersecurity

All News Images Videos Books More Settings Tools

infographic wallpaper healthcare defense in depth landscape government

Cybersecurity in the age of mobile ...
thenextweb.com

10 cybersecurity trends to expect in 2018
ifsecglobal.com

Cyber-security: A necessary component ...
globalrailwayreview.com

Why We Need More Women in
tripwire.com

Cybersecurity Startups Struggle To Keep ...
pymnts.com

Cybersecurity: Common Risks - Strategic ...
sfmagazine.com

Cybersecurity - Washington University ...
engineering.wustl.edu

Go to Google Home
newsroom.cisco.com

REAL PEOPLE ARE AFFECTED

The field of cybersecurity is a relatively new one, constantly evolving and full of complex problems. These problems affect real people in significant ways. Data and financial information are being siphoned through phishing operations and large-scale breaches like Equifax. The WannaCry ransomware attack shut down 30% of U.K. hospitals, causing hours-long delays, when seconds and minutes cost lives. Disinformation campaigns impact the way people vote and contribute to growing social division. Malware like NotPetya has shut down global shipping operations and disrupted national economies. Journalists need to keep their sources (and themselves) safe, but ensure those sources are who they say they are. Activists need to protect themselves in dangerous situations or otherwise face consequences like imprisonment, torture, and death. The list goes on.

WHY IT MATTERS

Since technology is ubiquitous in society, cybersecurity has become an increasingly important topic for many actors, from businesses to civil society to governments, and beyond. And with that, there are a slew of inspiring innovations, cybersecurity heroics, and people with rich stories about how they inform or are affected by this world.

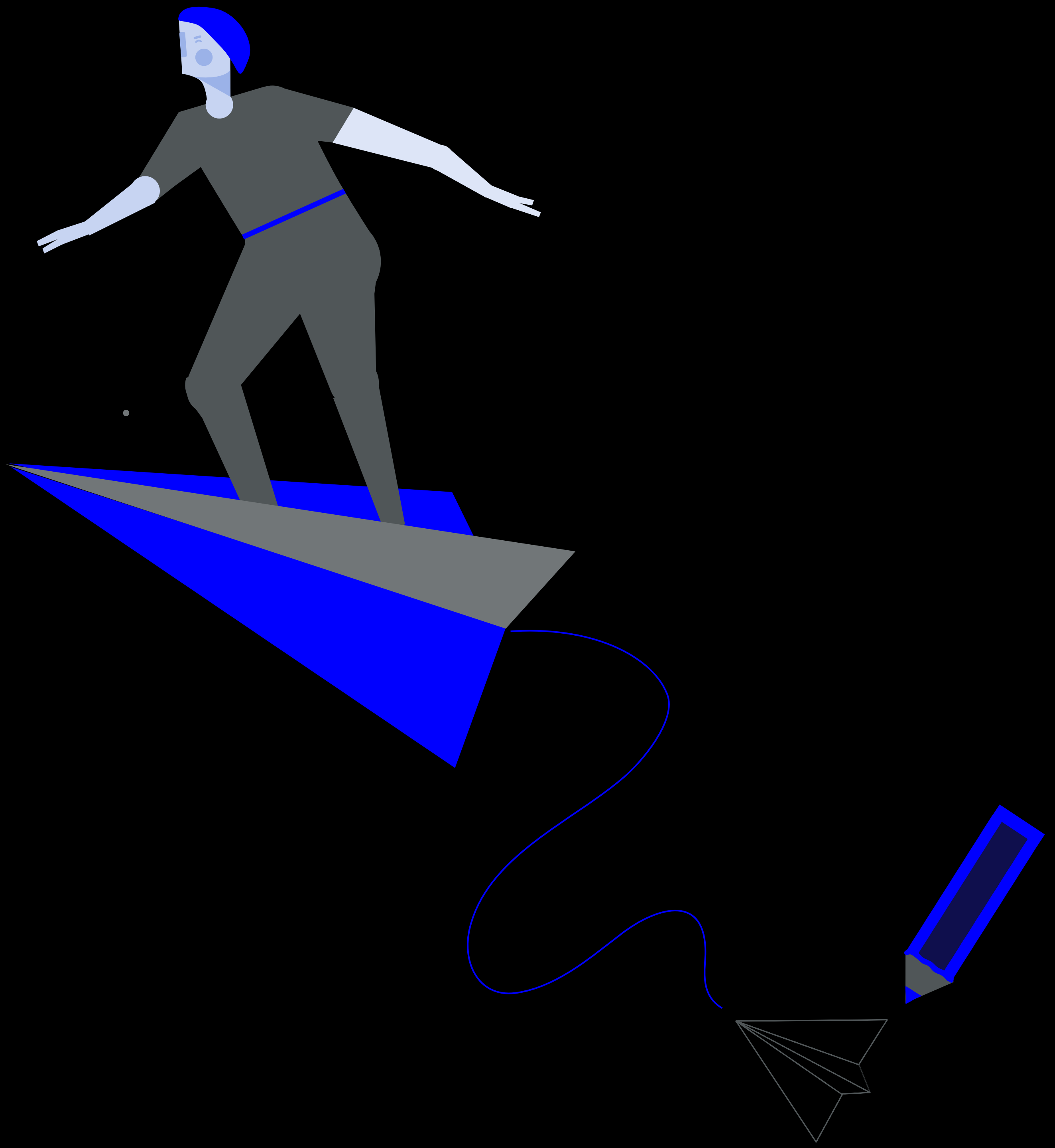
However, all too often, those stories about real people and innovation are dismissed, misunderstood, or ignored altogether in favor of fear-mongering or sensationalism. Rather than thinking about whether our devices are ones we can trust — a concept with which the average person can relate — we become mired in the concept of “security.” In doing so, the complex trade-offs societies make among our need for privacy, quest for security, and desire for innovation, are ignored. This leaves a divide between technical experts, who can tell countless nuanced stories of cybersecurity, and those in power who can make changes in the space (such as policymakers), who are often on the receiving end of a narrative full of fear, uncertainty, and doubt.

Kelsey Wroten, a visual creator who participated in our New York City group session, designed this piece that builds on her editorial illustration experience.

THE ROLE OF VISUAL CREATORS

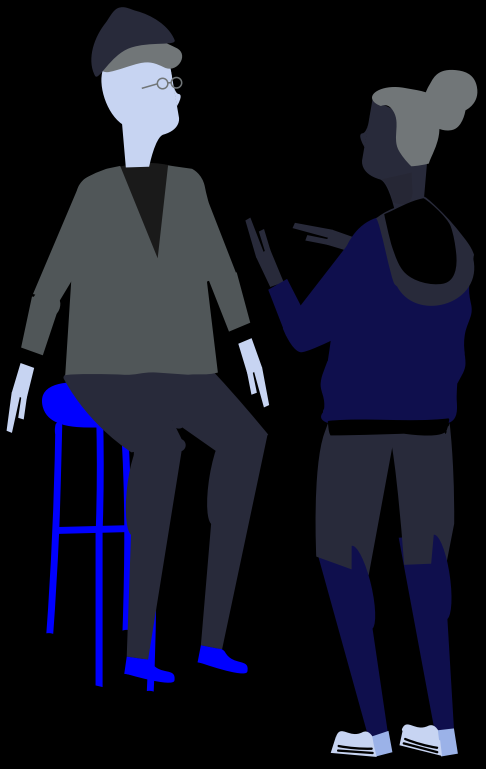
We need to find new ways to communicate about cybersecurity. This report starts bridging the divide between technical experts and decision makers by leveraging the power of visual design. As designers, we know that visuals help us translate information in accessible ways. However, the images we create need to be clear, compelling, and have solid technical underpinnings, as there are very real dangers when visuals are not built with the right foundation.

Cybersecurity needs more creators who can collaborate with experts on the future aesthetics, brand, direction, and visuals for the space. With a mix of creativity and collaboration, there's an opportunity to change the future of this field and open up a rich, important conversation to more people who need to know about it.



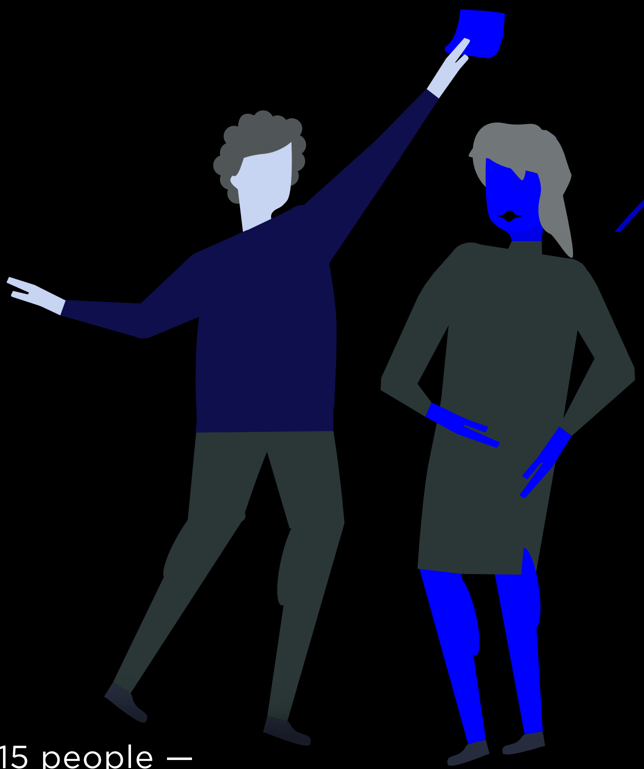
APPROACH

For this work, the OpenIDEO team, with support from the Hewlett Foundation's Cyber Initiative, which commissioned this report, embarked on two months of dedicated research. We focused on capturing needs and insights from experts, influencers, and decision makers in the cybersecurity field, and identifying the tools necessary to equip visual creators to responsibly, effectively, and innovatively design for this space.



Interviews

Individual, multiple-hour conversations that mixed questions and observation to uncover deep insights about the field.



Group Sessions

Groups of eight to 15 people — targeted around a specific persona — engaged in a mix of creative exercises and conversations.

Secondary Research

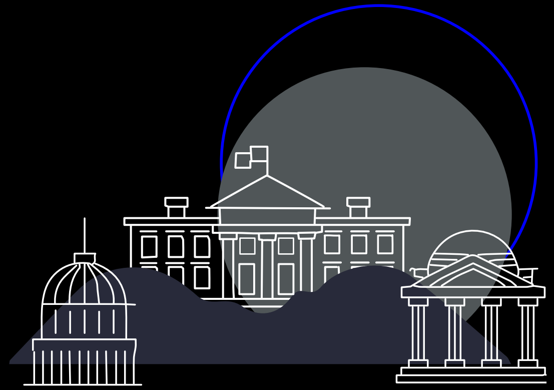
Additional research through reviewing articles, industry papers, media, and other documents.

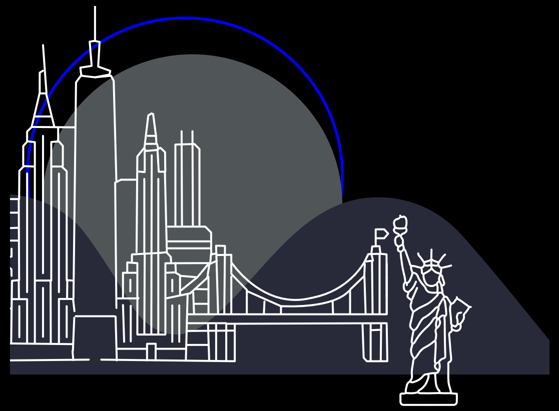
GROUP SESSIONS

You can come to a thorough understanding of a community's life, dynamics, and needs by conducting a group session. Though they may not offer the depth of an individual interview, they can give a closer look at the beliefs and behaviors of segmented groups of people who you're designing for. The best group sessions seek to hear everyone's voice, revel in the conversation, shine light on diverse opinions, and are strategic about group makeup. We assembled groups of eight to 12 individuals, in four cities, focusing on different topical angles in each city to uncover insights about the space and this work.

San Francisco, CA, U.S.A. Uncovered needs and opportunity areas from private sector and civil society subject matter experts.

Washington, DC, U.S.A. Learned about how decisions are made with policymakers, journalists, and other civil society experts.



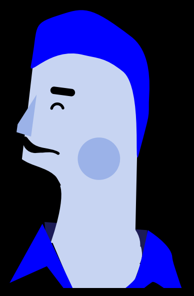


New York, NY, U.S.A. Tested what visual creators need to design for cybersecurity and prototyped visual assets.

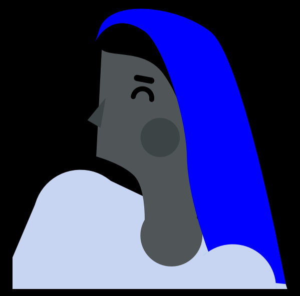
Nairobi, Kenya. Tested what visual creators need to design for cybersecurity and prototyped visual assets. Helped challenge our Western biases.

INTERVIEWS

We like to observe real people and talk to them to uncover insights. Our interviews were usually multiple hours and involved an array of creative exercises. We developed diverse “personas” to help select people to interview and gather a range of perspectives. On the right page are the personas for the 10 in-depth interviews we conducted.



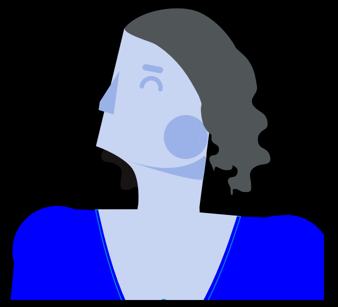
Hackers. Tinkerers who attack or protect others. It’s now a professionalized space with commercial, nation-state, and criminal actors. We need to move away from the stereotypes of an individual in a basement.



Subject Matter Experts. Those who have been working in the cybersecurity space for years and bring technical and contextual knowledge.

Visual Creators. People who could design the visuals that will be used in the space. Few of them have cybersecurity expertise.

Analogous Inspiration. Cybersecurity isn’t the first field to undergo a visual overhaul. What can we learn from other complex, multidisciplinary spaces?

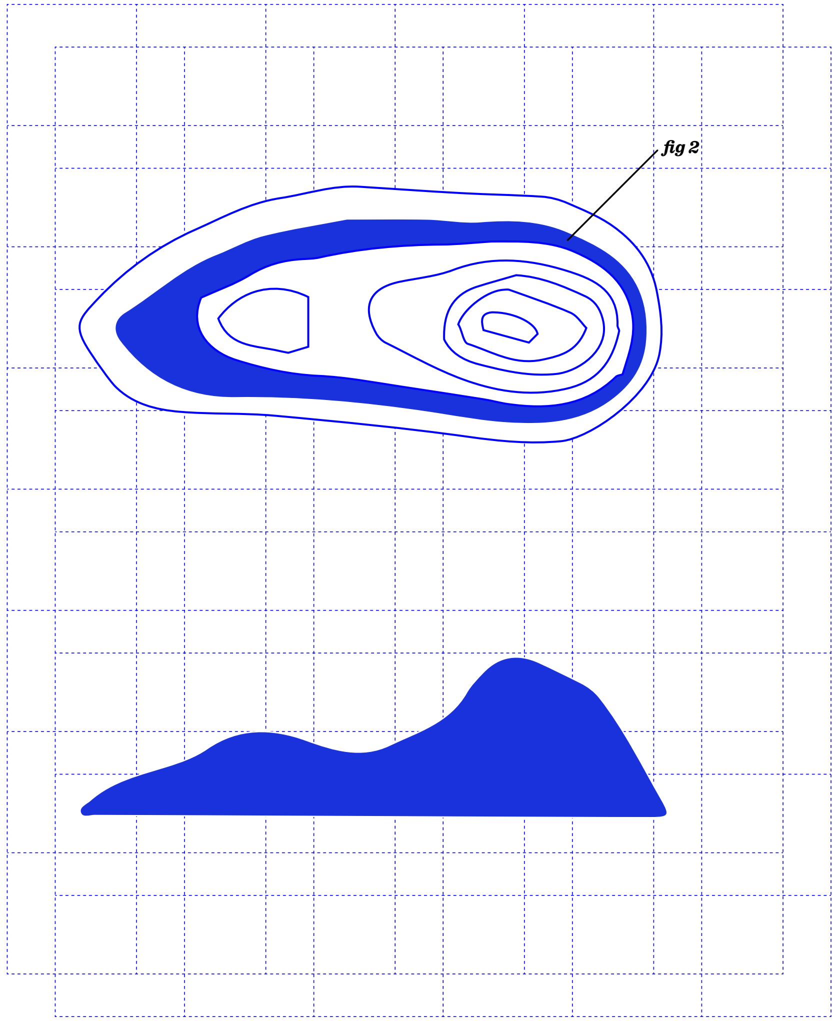


Journalists. Folks who write stories about cybersecurity, and image editors that select visuals to accompany them.

Policymakers. These individuals make large policy decisions around cybersecurity — in tandem with experts — but often lack deep technical expertise themselves.

SECONDARY RESEARCH

The team entered this project with respect for the work that so many organizations and designers have already done around visuals in the cybersecurity space. We sought to learn from previously conducted research and a landscape analysis of how organizations are already designing visuals in this space.



Chapter 2

DESIGN PRINCIPLES

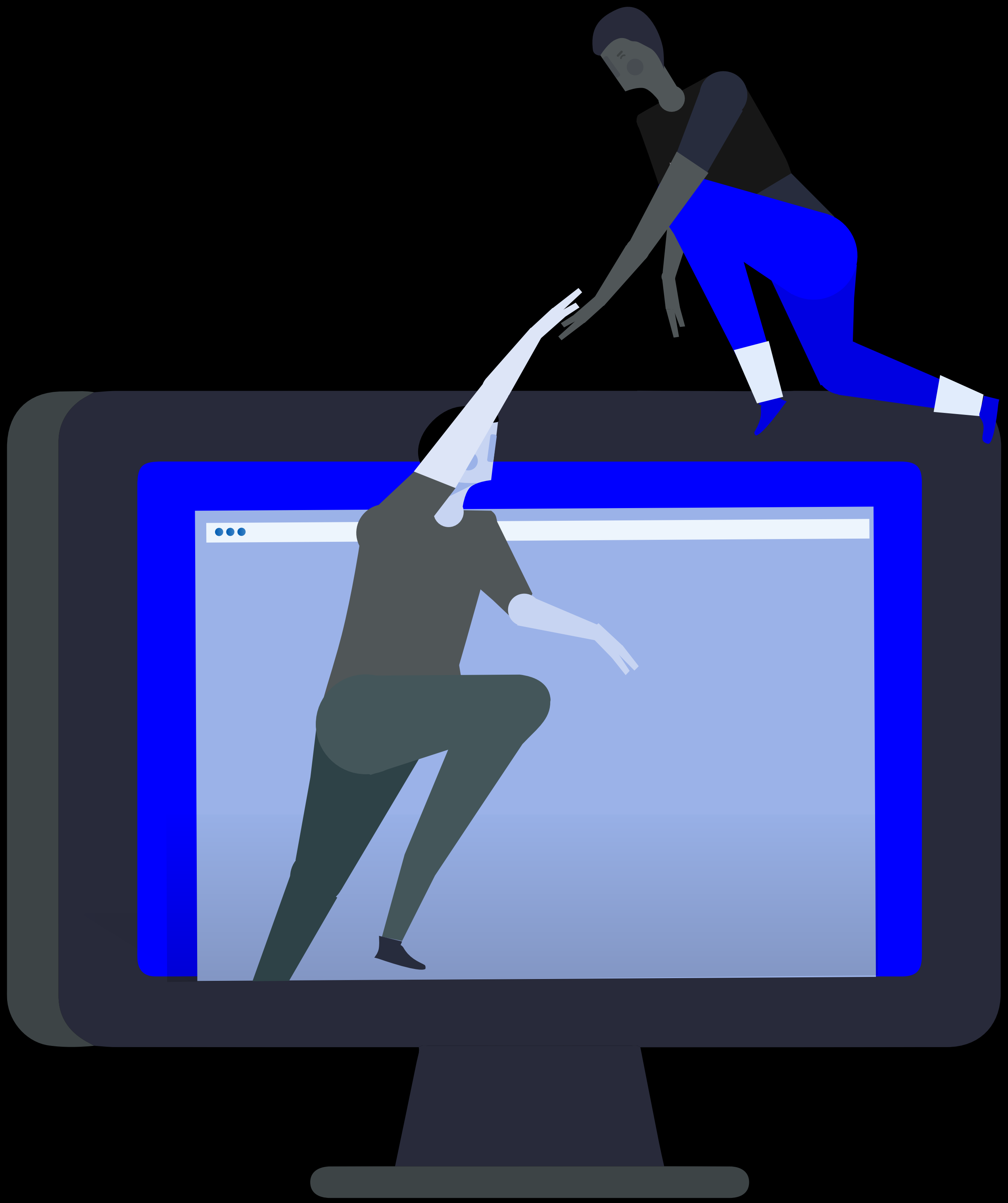
As we build visuals for cybersecurity, there are unifying elements that can serve as our guidelines. Design Principles help us develop visuals that are centered around what the cybersecurity space aspires to be. Informed by our research, these principles can provide visual creators with the guidance to design with empathy in this space.

Design Principle 1

HUMANIZE THE SPACE

Current cybersecurity visuals showcase circuit boards, server racks and rooms, and anonymous men in hoodies. However, this doesn't represent what is a very human issue. It is people that make the circuit boards that get compromised, people who get hacked, and people who work to secure our technology and systems.

> *"We need to get people to understand that these are moments that begin with a keyboard and end in the physical world."*
>
> — David Sanger, national security correspondent, *The New York Times*



Design Principle 2

INSPIRE HUMILITY THROUGH ACCESSIBILITY

Cybersecurity (and technology more generally) can be full of complex information. This is a relatively new and growing field, and even subject matter experts acknowledge the constant evolution in the space. When visuals are accessible, people are able to concretely understand a technical topic, and will hopefully be inspired to learn more about the subject.

> *"Cybersecurity is not a basic literacy that people have."*
>
> — Ryan Calo, University of Washington Tech Policy Lab

Design Principle 3

RAISE THE ALARM, BUT DON'T BE ALARMIST

Many existing cybersecurity visuals induce fear, uncertainty, and doubt in their audience. Multiple individuals working in cyber policy with U.S. government shared that this can be dangerous, as fear-inducing narratives distract decision makers from root causes and systemic issues. Since there are already an assortment of fear-inducing images in the wild, many practitioners are searching for visuals that evoke a different narrative about cybersecurity. We seek to bring in new elements like hope and trust to visuals, while avoiding false or blind optimism.

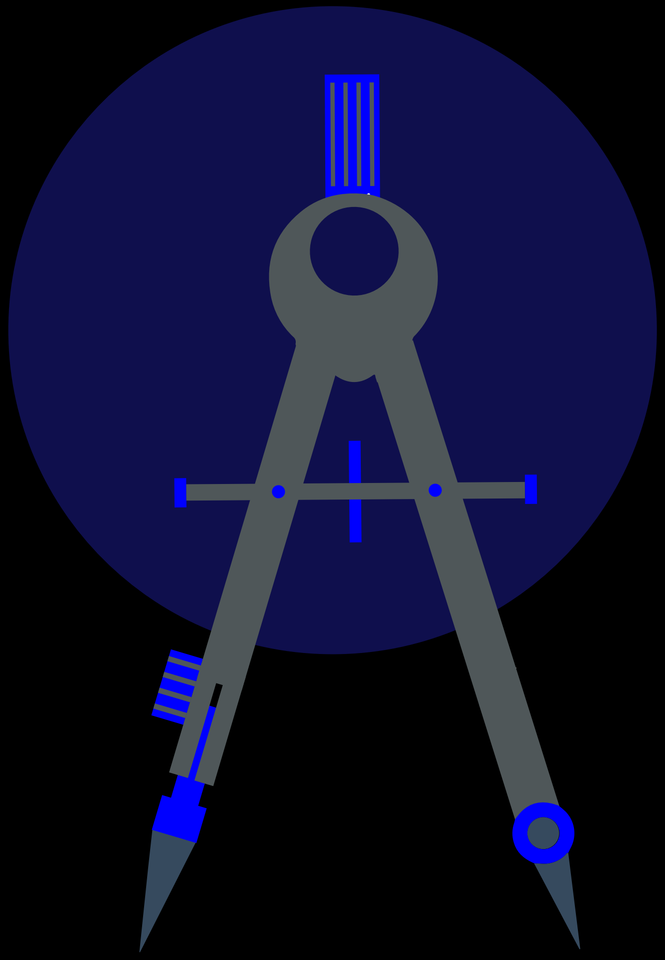
> "FUD" (Fear, Uncertainty, Doubt): This is present in many of the visuals in the space. Rather than aiming for FUD, it's important to ground in reality, balancing the urgency of an issue, but avoiding an apocalyptic message with the sole purpose of instilling fear.

Design Principle 4

ACCURACY BUILDS CREDIBILITY

It's important that the visuals we create incorporate real, technical expertise. They should be grounded in how cybersecurity actually works. Experts in the space report that visuals that don't accurately convey the facts about cybersecurity can lose credibility among certain audiences and, in some instances, contribute to dangerous misconceptions and narratives.

There is a tension in this field between making an image relatable to the average person and providing the technical accuracy that satisfies cybersecurity experts. This tension may not be entirely on visual creators to solve. The resolution will depend on a shift in mindset on the part of technical experts to accept visuals that are not as technical as those exhibited in journal articles, but are still accurate enough to engage the public without deeply misinforming them.



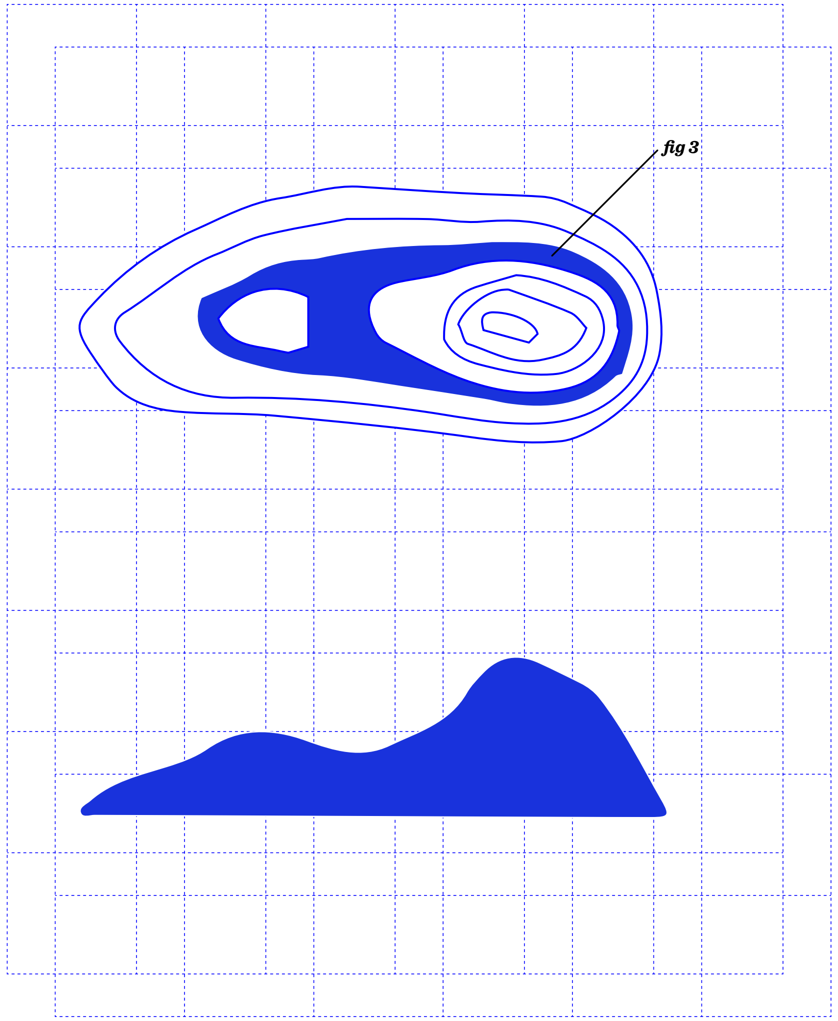
A recent article in *Bloomberg* went into detail about how China used a tiny chip to infiltrate the U.S. technology supply chain, allegedly affecting almost 30 U.S companies. However, cybersecurity experts we spoke with heavily criticized both the substance of the article and the visuals within it. While the visuals were eye-catching, *Bloomberg* lost credibility when other companies involved denied the story, and other journalists weren't able to confirm it. It's one of many examples showing that accuracy builds credibility.

Design Principle 5

MAKE THE INVISIBLE VISIBLE

When it comes to cybersecurity, a lot of elements are not tangible. Take healthcare as an analogous example: We can feel when we are sick and see the instruments that fix us, but need help understanding the diseases that make us ill. Visual designers are needed to bring tangibility to terms like the internet, encryption, or privacy.

> *"Cyber is inherently intangible. There are only so many glowing keyboards you can show."*
>
> — Ryan Evans, editor-in-chief of web magazine *War on the Rocks*



Chapter 3

MINDSETS

Human-centered design is as much about your head as your hands. These mindsets explore and uncover the philosophy that visual creators should adopt to best design for cybersecurity. Coming directly from our research, we believe these will support designers with building effective and useful creations for the space.

Mindset 1

OPTIMISM

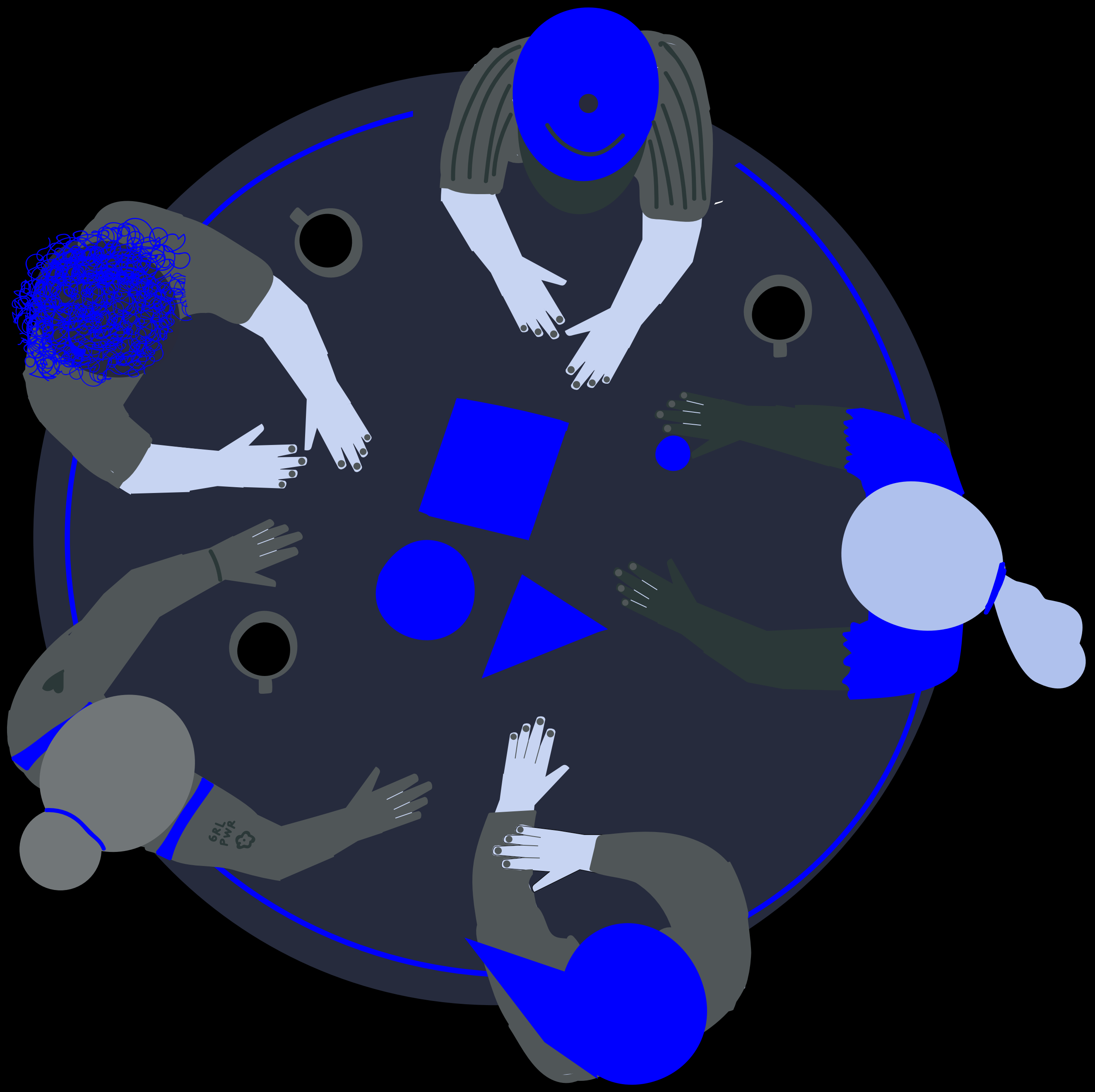
We met passionate cybersecurity practitioners who are working tirelessly to support people in this space. Many of them hit roadblocks consistently, have trouble seeing and conceptualizing the progress they've made, and are on the verge of burning out. Meanwhile, the images in the space are often built on a narrative of fear. Many of those with whom we spoke expressed a desire to introduce visuals that are created from a place of hope and positivity.

> *"One of coolest interactions I had at DEF CON was with little kid named Emmett Brewer...He was able to hack mockups of an election result page in 10 minutes. He was articulate and thoughtful...and stands out as one of the people who gives you hope for the future."*
>
> — **Stephen Hiltner**, reporter and photographer at *The New York Times* (also credited for the photograph of Brewer on the right page)

Mindset 2

CO-CREATE

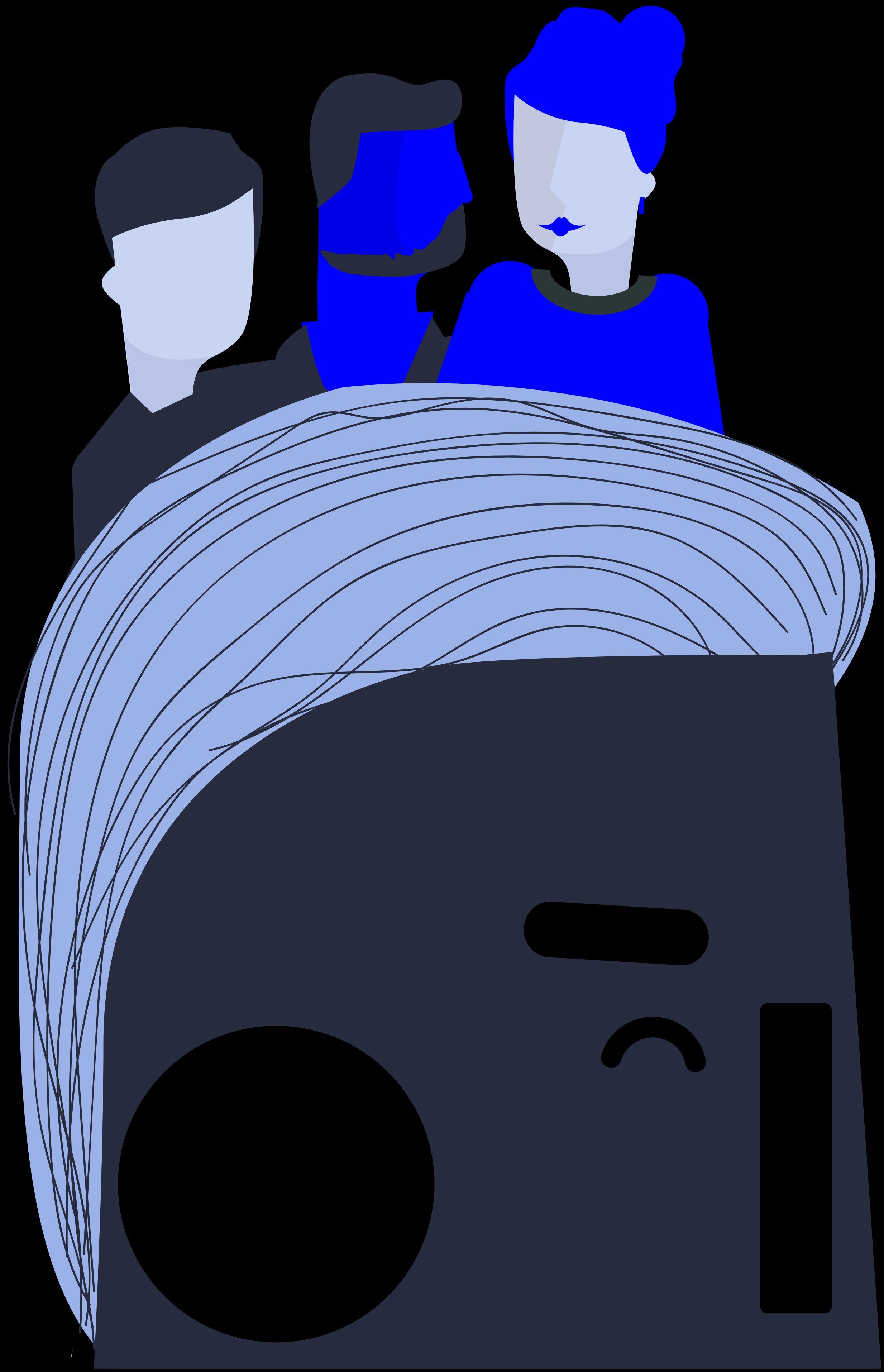
Visual design shouldn't be created in isolation. We need to work in partnership with cybersecurity experts to further refine our designs. It's important to get their feedback early on in the process. Images need to resonate with these technical experts who have deep knowledge in this space, and they can ensure the facts are directly tied to the visuals we create. By co-creating, we ensure visuals are credible, avoiding counterproductive or even dangerous outcomes.



Mindset 3

EMPATHY

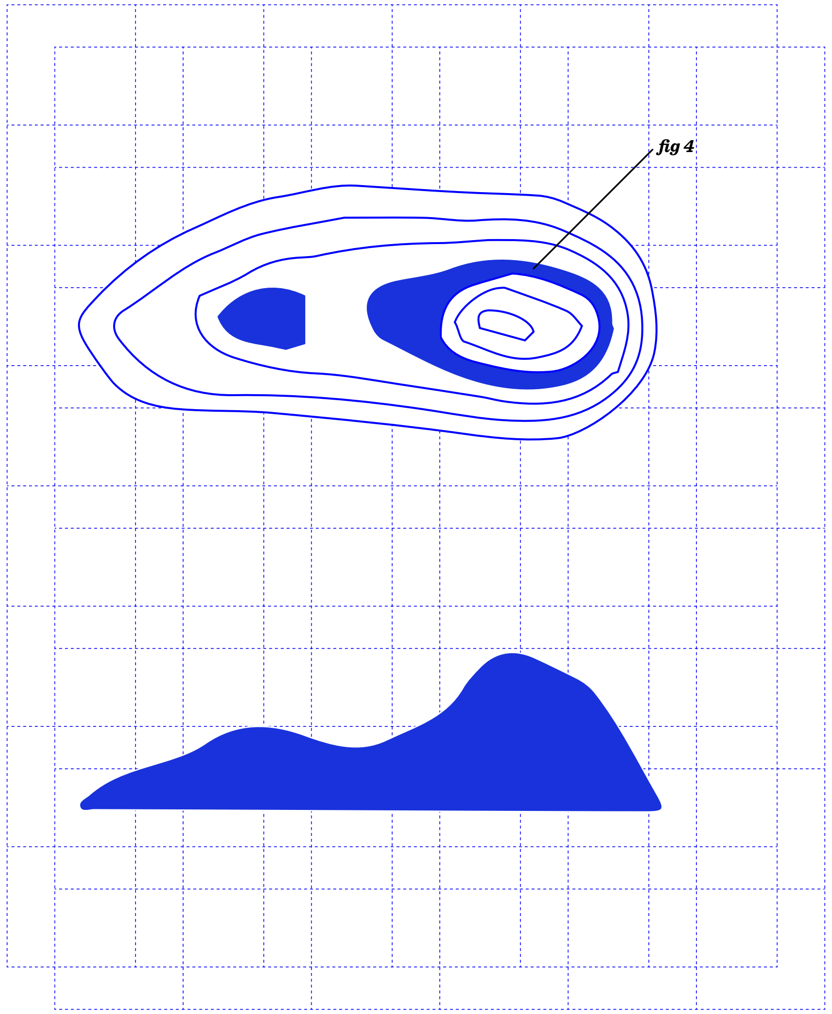
As visual designers, we're going to be most inspired when we immerse ourselves in the communities we're designing for. From those immersions, we recall conversations, moments, and spaces; with that input, we design visuals. By learning more about cybersecurity, we can design more effectively and truthfully.



Mindset 4

FOCUS ON NARRATIVES

When it comes to cybersecurity, designers have the opportunity to change the mindsets and behaviors of decision makers and the general public. Visuals should be rooted in compelling stories, and there should be a reason behind each element that's included.



Chapter 4

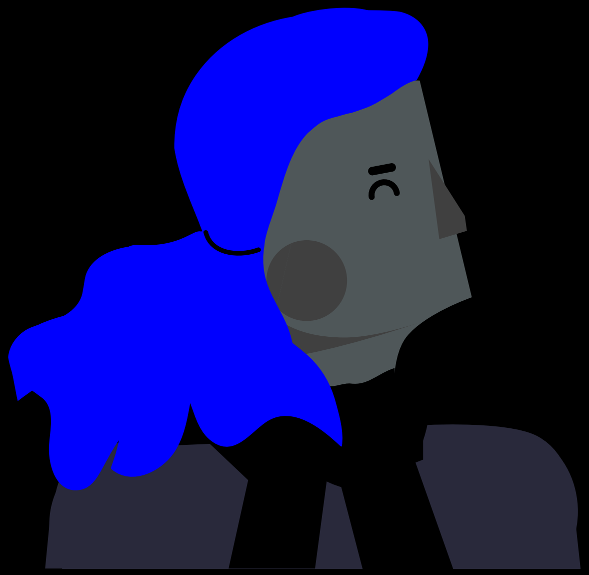
BRAND STARS

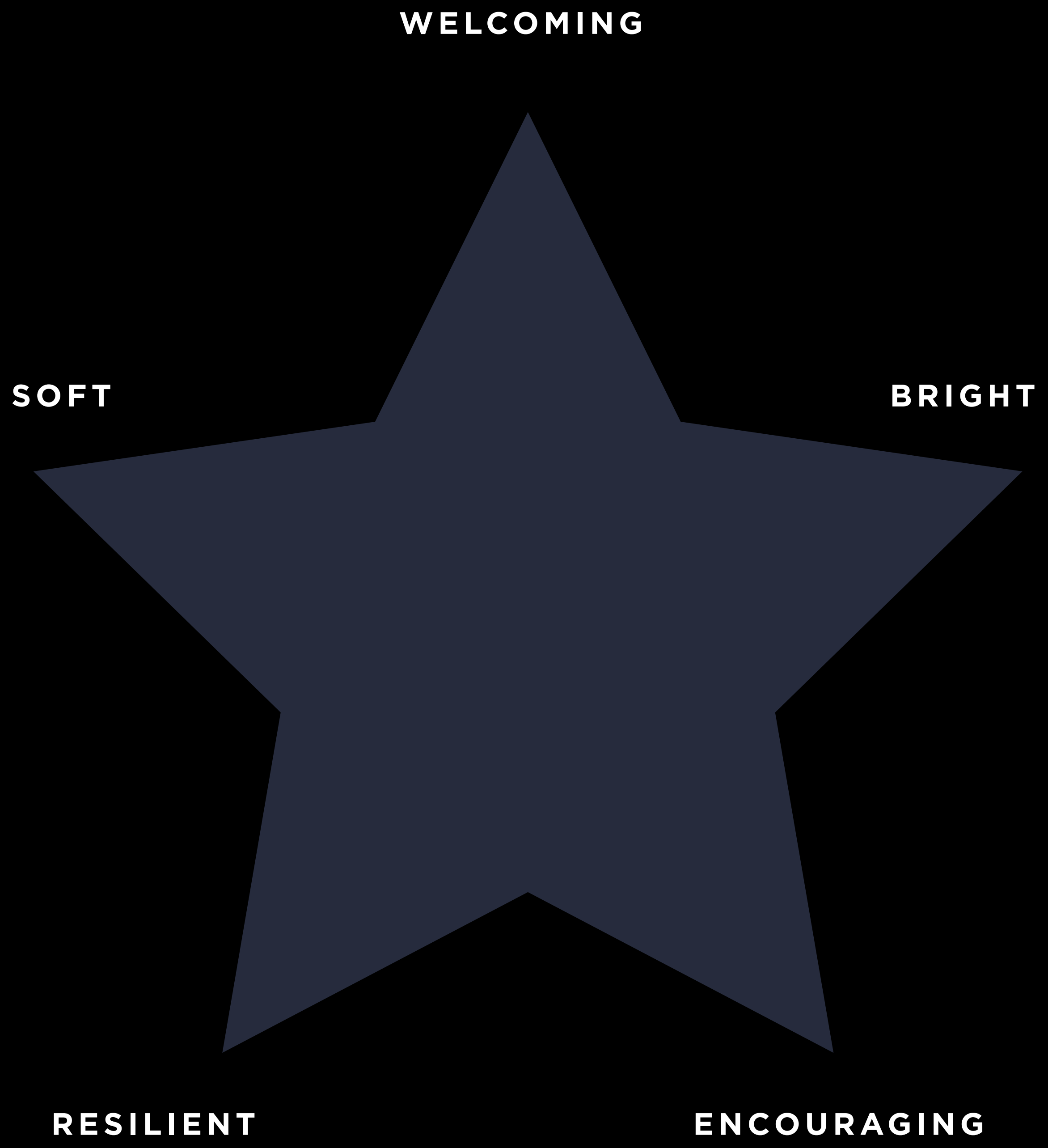
Brand stars help us define the personality of a brand or space. This tool helps visual designers understand how their creations “feel” in the world. We offer a number of different stars, based on the personalities and needs of those we met in our research. These stars should help create guidelines and alignment for the visuals created in the space, while also serving as a source of inspiration.

Brand Star 1

HUMAN
ETHOS

Bringing humanity into the visuals we design has been a need expressed by those we interviewed. This brand star will help you create visuals that are softer, warmer, and have a human element to them.

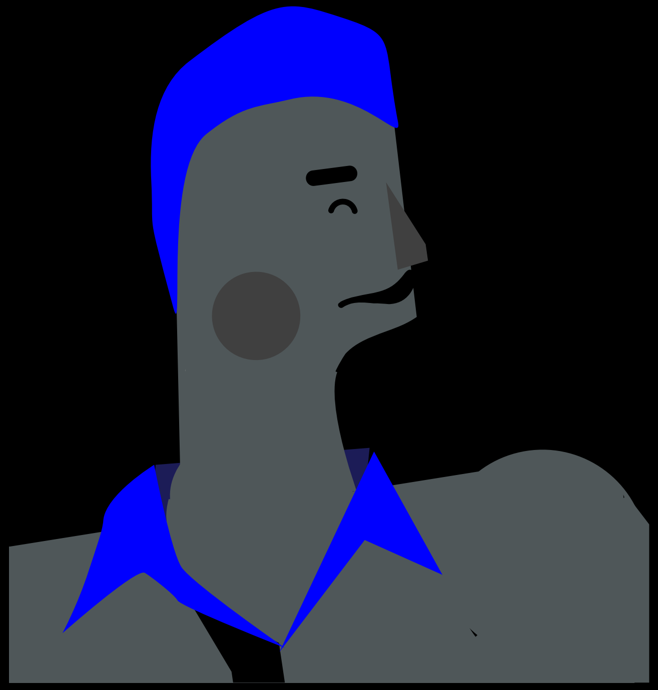


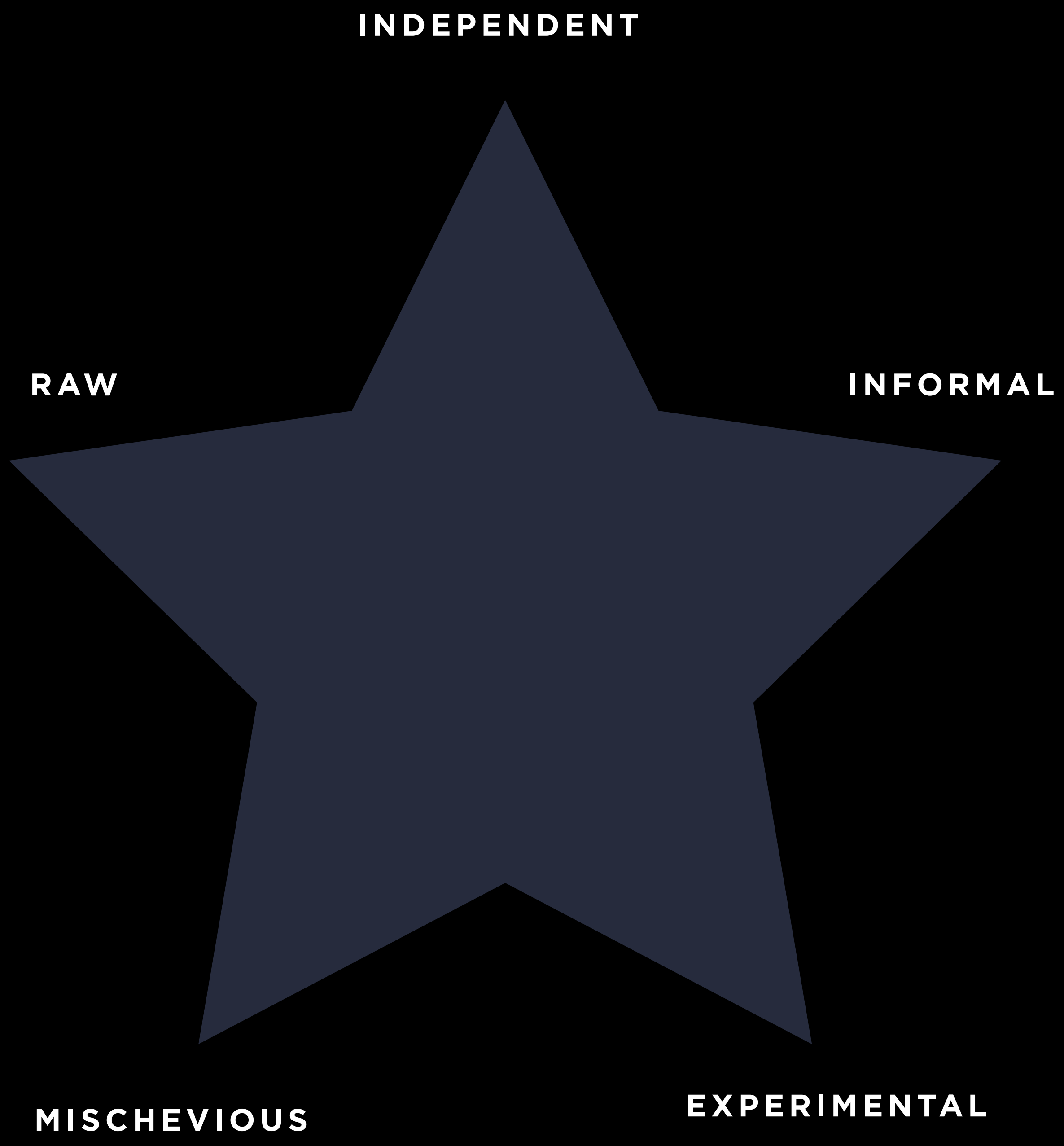


Brand Star 2

HACKER ETHOS

There isn't just a single kind of hacker, and we want to move away from stereotypes. This brand star will help you create from the overall culture and ethos of hackers, which tends to be scrappy and raw.





INSPIRATION

When we first started this project, we fell into a trap: thinking of hackers as a single group of people. We imagined a guy in a basement who did nefarious things with our credit card information. While there may be a few who fit that stereotype, the hacking community is truly much more diverse.

There's a professionalization that has happened within the hacking space — some work commercially or for the government, others are part of large criminal enterprises or nation-state efforts. There are also those who "hack for good," using their talents to end child abuse or sex trafficking rings, for instance. During our research we discovered five potential motivational profiles for hackers developed by I Am The Cavalry, a grassroots cybersecurity organization. It expanded our perspective of hackers. We hope they inspire your work as well.

Protectors

Make the world a safer place. These hackers are drawn to problems where they feel they can make a difference.

Puzzlers

Tinker out of curiosity. This type of hacker is typically a hobbyist and is driven to understand how things work.

Prestige

Seek pride and notability. These hackers often want to be the best or very well known for their work.

Professionals

To earn money. These hackers trade on their skills as a primary or secondary income.

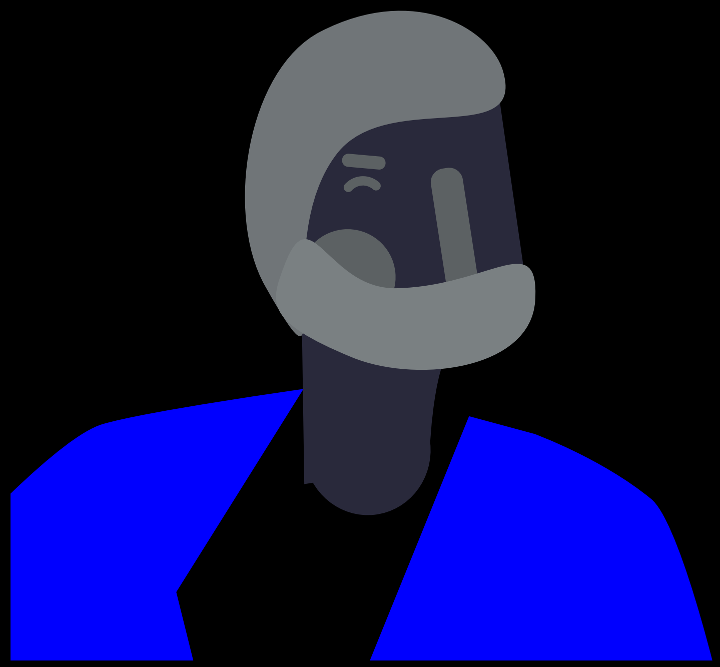
Patriot/Protesters

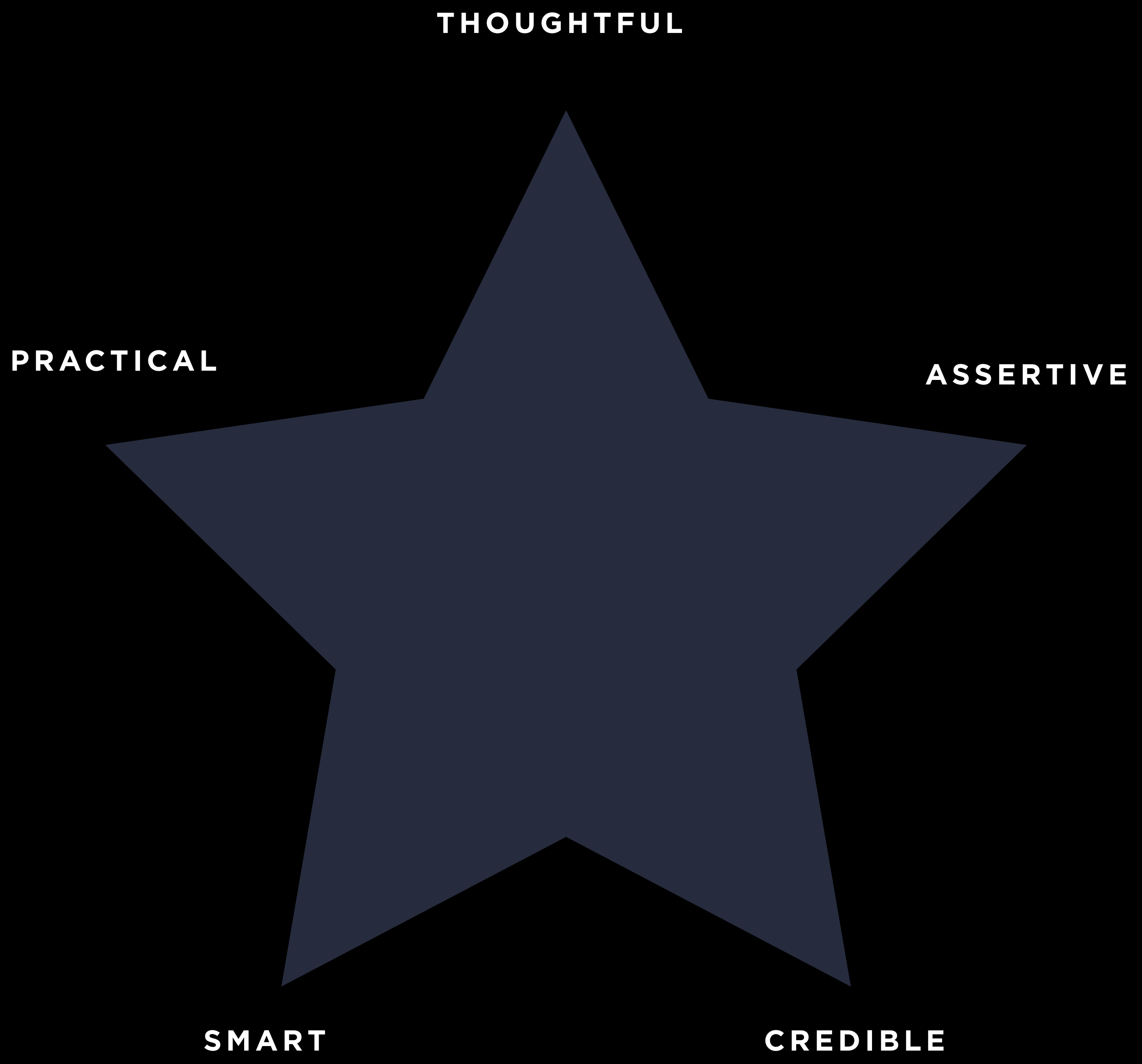
Ideological and principled. These hackers, whether patriots or protestors, strongly support or oppose causes.

Brand Star 3

EXPERT ETHOS

Visuals that communicate expertise are important in building credibility with some audiences. We've learned in our design research that people pay close attention to the way a visual feels, what it says, and the technical rigor behind it. This brand star will help you create from that place of thoughtfulness and practicality.





THOUGHTFUL

PRACTICAL

ASSERTIVE

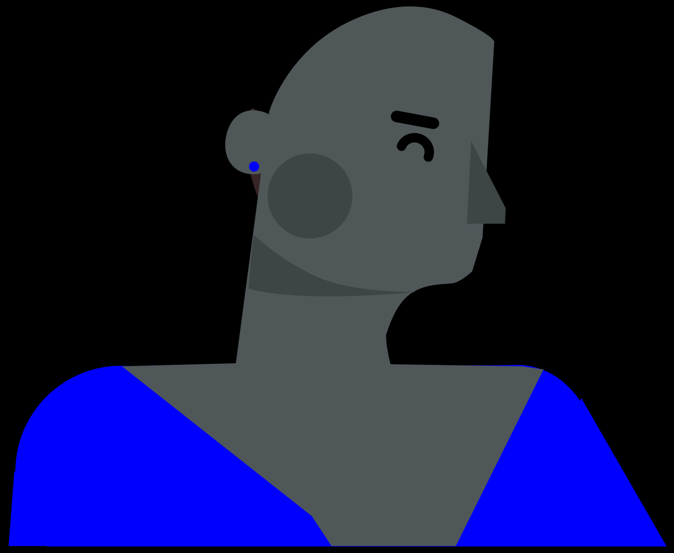
SMART

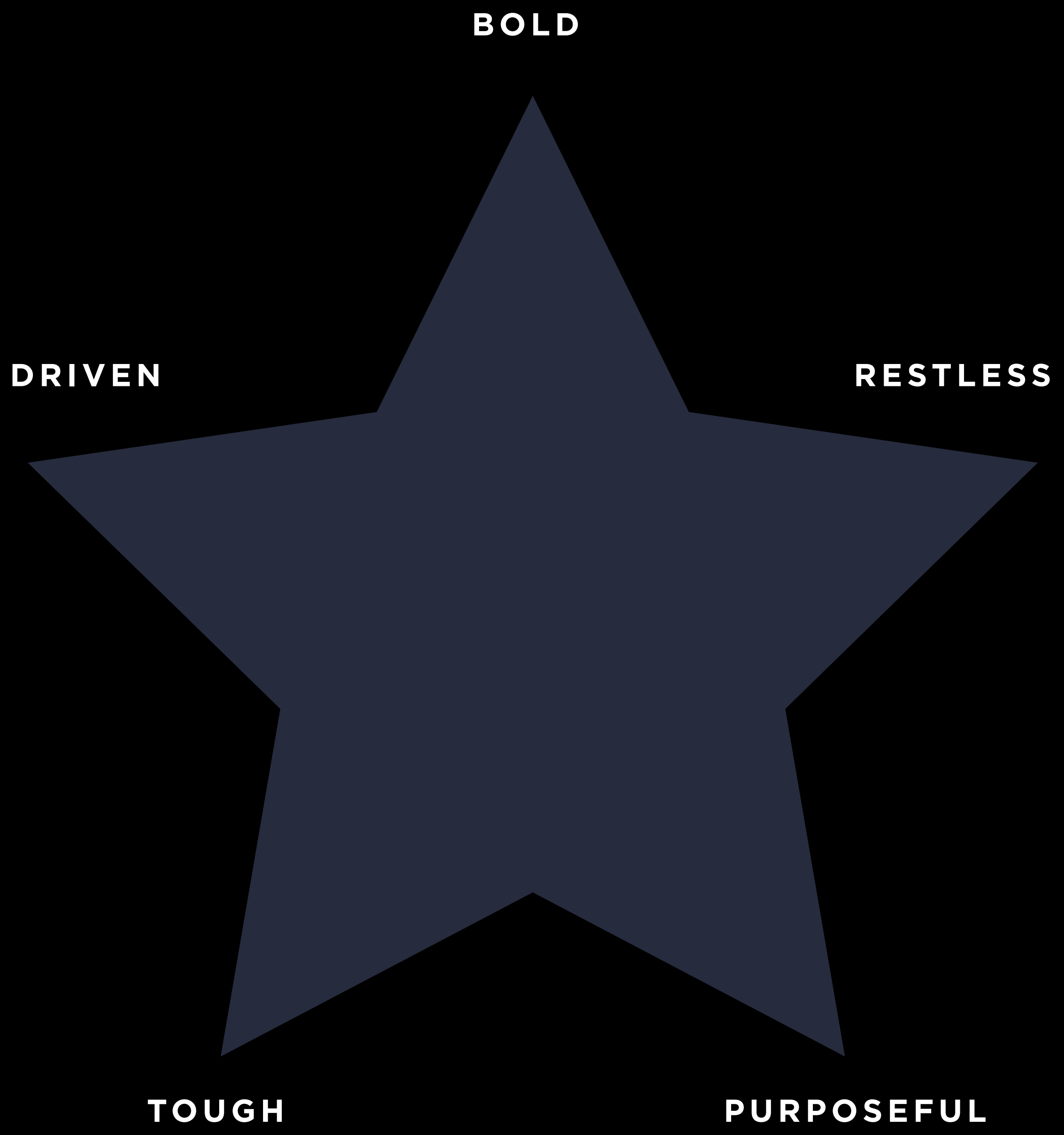
CREDIBLE

Brand Star 4

DEFENDER ETHOS

The word “security” is an important part of a visual. Many who engage in this work come from corporations or governments and are trying to protect their clients and citizens from criminal enterprises and nation-state violence. This brand star will help you create from that place of thoughtfulness and practicality.



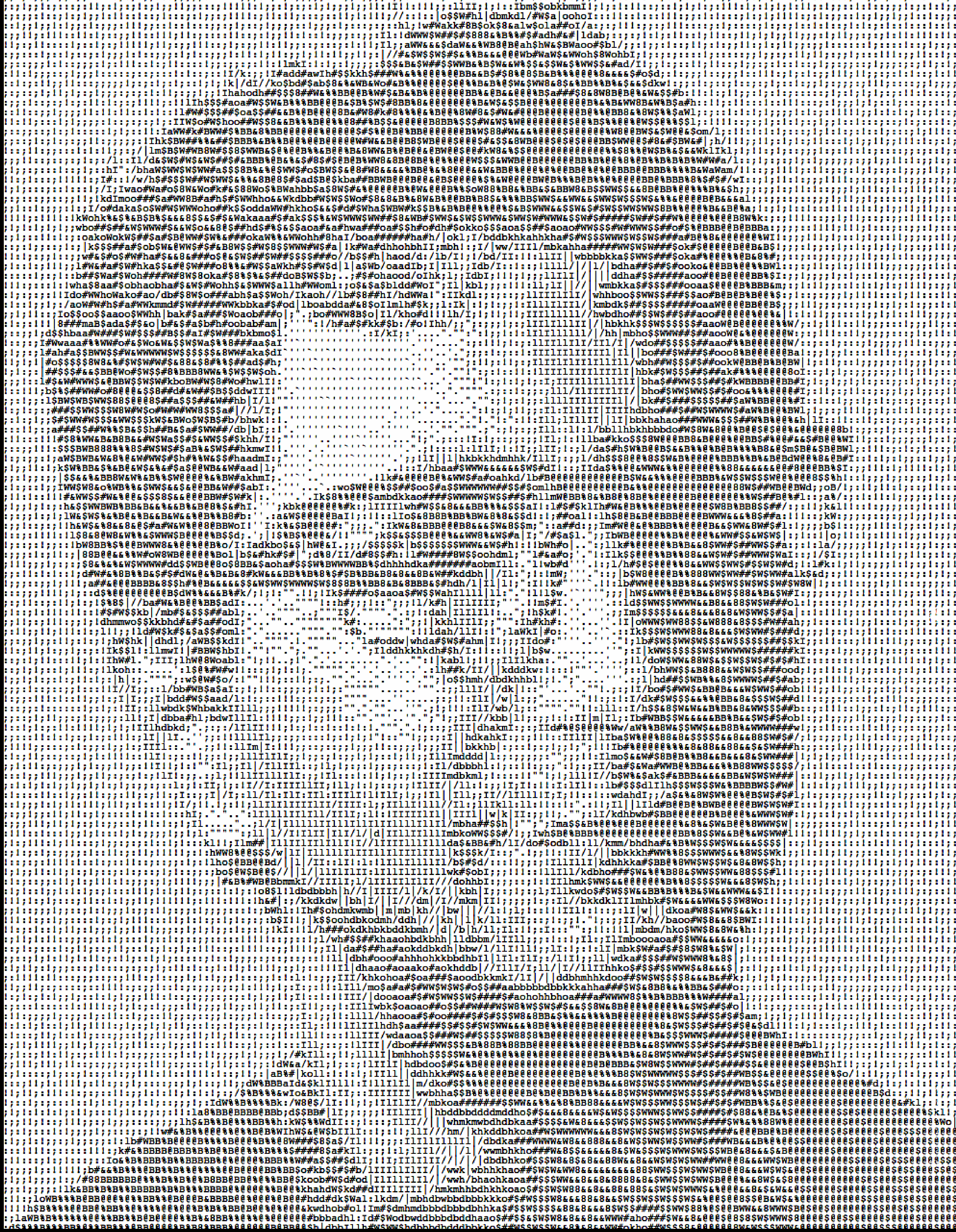


ANONYMITY

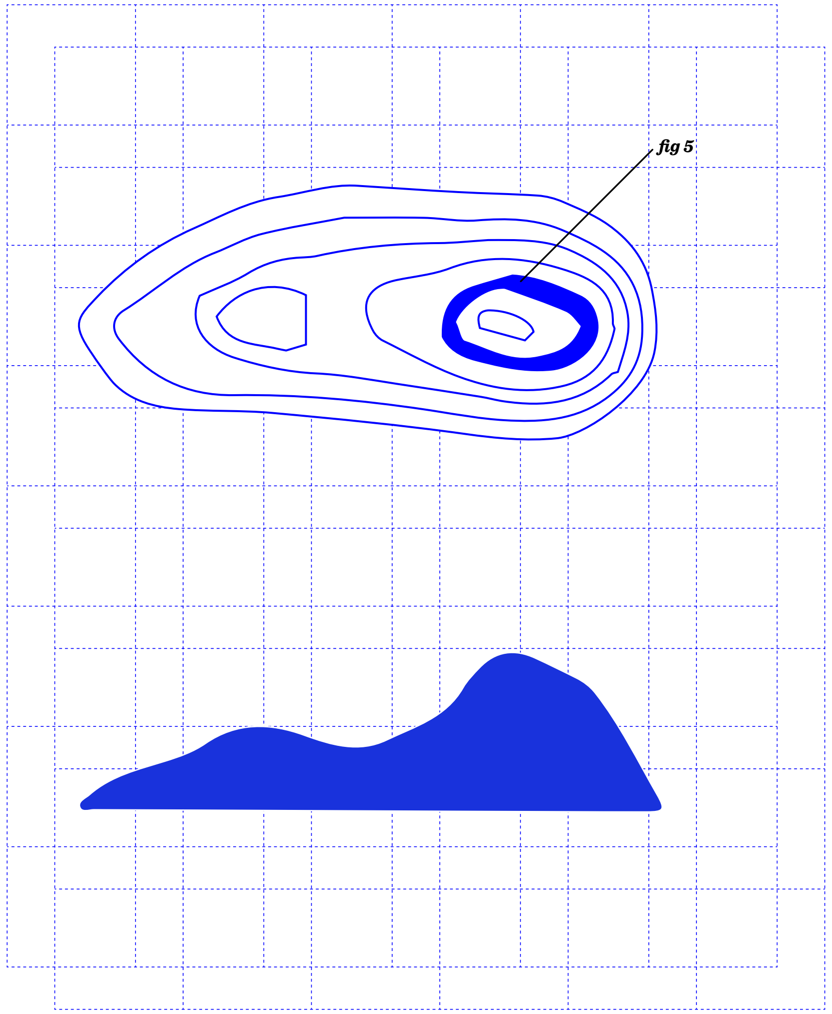
Stephen Hiltner, a writer-photographer for *The New York Times*, wanted to protect the anonymity of the hackers he was covering at the annual DEF CON conference. The nature of their work and their lives often calls for such discretion. His goal for the piece, "For Hackers, Anonymity Was Once Critical. That's Changing," was to bring an element of humanity to those he met, without compromising their identity. So he chose to shoot their portraits in black and white, and use an animator created by two colleagues to convert his photographs into ASCII art.

What is ASCII art? This graphic design technique uses keyboard characters to piece together a larger visual. The ASCII animation morphs a photograph enough to prevent identification, while still keeping a touch of humanity.

We wanted to highlight this as an example of a visual technique used when featuring stories of specific humans whose identities need to be kept secret.



Jeff Moss, the founder of DEF CON, was photographed by Stephen Hiltner/*The New York Times*. The black-and-white photo was turned into ASCII art by Aaron Krolik/*The New York Times*.



Chapter 5

A-HA! MOMENTS

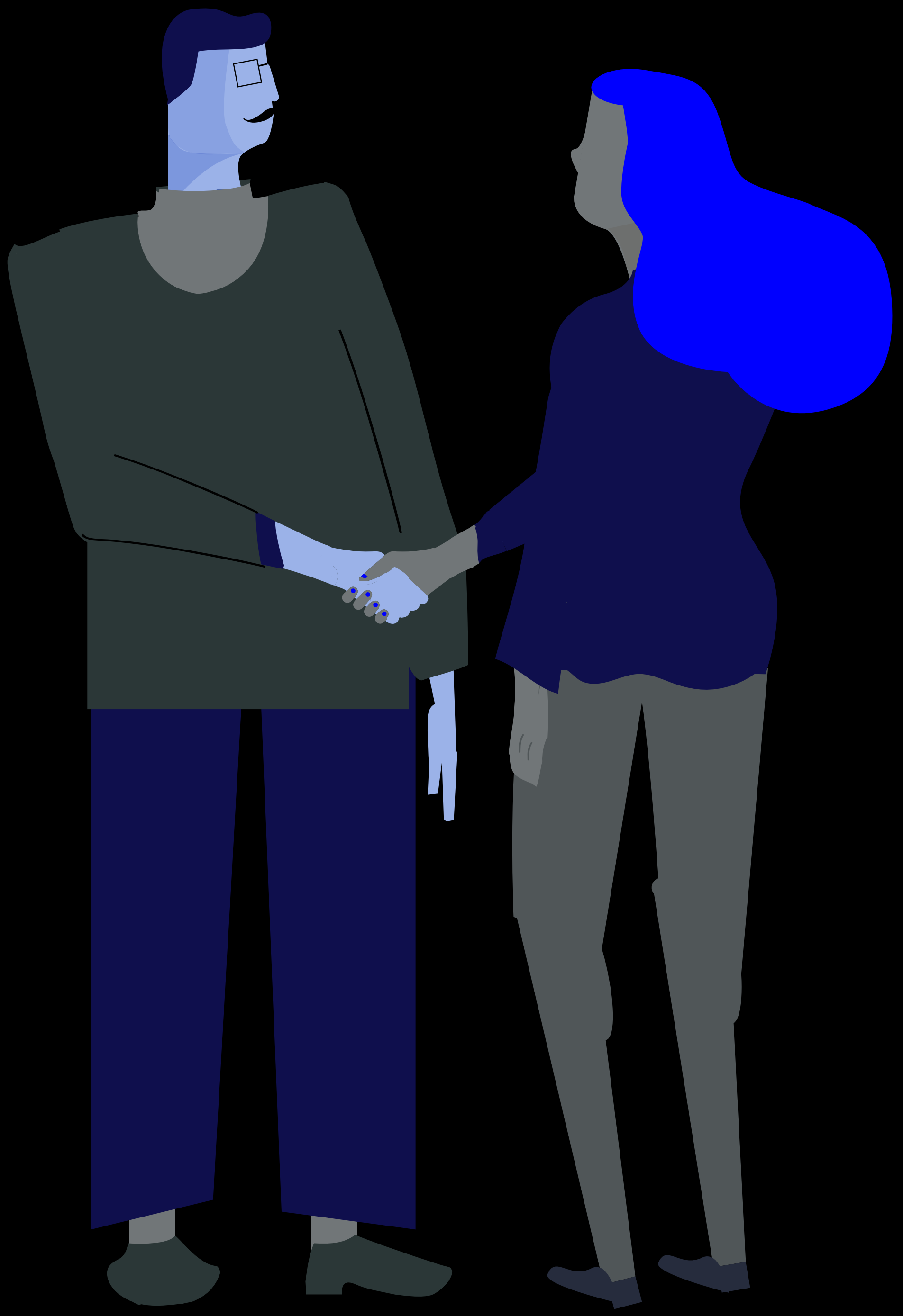
As we navigated through our group sessions, interviews, and secondary research, a series of insights surfaced again and again across individuals and sectors. These insights, which we call "A-ha! Moments," are a window into the problems and questions facing the cybersecurity community.

A-HA! Moment 1

PEOPLE WANT TO FEEL LIKE THEY CAN WIN

The issues facing cybersecurity don’t currently feel like ones we can overcome. They feel so big and so complex that people can’t comprehend how even the smallest individual step could make a difference. There is a hopelessness around the field, married with enough jargon that the average person can’t pick apart issues to understand from where hope could spring. How can we break down cybersecurity issues so they feel manageable and then empower people to tackle them?

> *“There’s a perception that we’re ‘losing’ — whatever losing means. People can get to a point where they say, there’s nothing I can do about it, so why even try?”*
>
> — Jeff Greene, vice president, global government affairs and policy, Symantec



A-HA! Moment 2

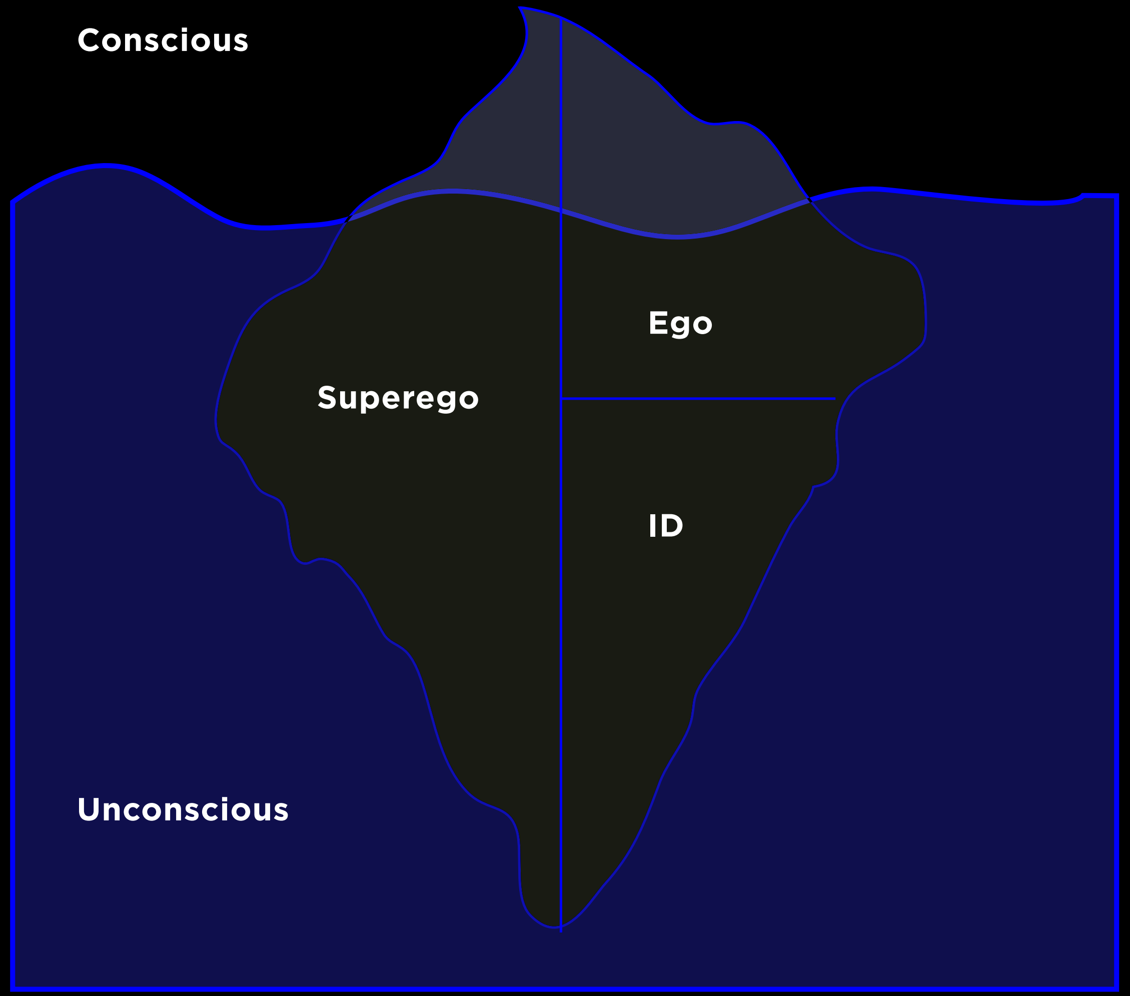
DEFINITIONS VARY, LET'S LEARN FROM THAT

While many subject matter experts and influencers we interviewed were aligned on the issues and terms that could use new visual representation, we rarely found established definitions or alignment around the definitions of those issues and terms. While these varied definitions can prove to be a challenge for many, the conversation about differing definitions, and the process of listening to experts talk about where and why they vary, can be invaluable information for visual creators as they seek to understand the nuances of the space.

A-HA! Moment 3

POWER OF ANALOGIES AND METAPHORS

Across fields, metaphors and analogies help with translation from abstract to concrete, or complex to simple. In our interviews, every cybersecurity professional used metaphors and analogies to further their work: from military professionals to technical experts working with legislative staff to hackers seeking understanding outside of their community. As with visuals themselves, it's important to create technically accurate metaphors, or at least understand and communicate the limitations of a metaphor, to prevent the spread of misinformation. Experts told us that some are overused, like nuclear security analogies.



Inspiration: A visual representation of Sigmund Freud's theory of the unconscious. What might be a complex psychological theory to some is made more accessible through an iceberg metaphor.

A-HA! Moment 4

DIVERSITY, EQUITY, AND INCLUSION

We've heard in interviews and group sessions that people don't feel the cybersecurity world is accurately being reflected in visuals created for the space. The cybersecurity field is rich with people we rarely hear about, of all age groups, races, and identities. This is not just about designing assets, but helping people feel like their communities are authentically reflected in the visuals created. As a byproduct of distributing diverse visuals, we hope to help attract more people to the field by making it feel more accessible and resonant in underrepresented communities.

> *"I'm tired of constantly searching Shutterstock for photos of women in cybersecurity and only coming up with silly images of women posing next to computers."*
>
> *— Elizabeth Weingarten, senior fellow at New America*

INCLUSIVE IMAGERY CHALLENGES ASSUMPTIONS

There is immense power and learning that can come from seeking the wisdom of experts outside your field. In an in-depth interview for this initiative, Sharon Lewis, director of the Afrofuturist film *Brown Girl Begins*, talked about how to focus on narratives that challenge people's assumptions.

Afrofuturism tackles stereotypes by visually portraying people in new ways.

> *"Afrofuturism is the perfect storm of technology and African history. Seeing those two things together that we never get to see. White people are usually associated with tech and people of color are portrayed as starving natives in Africa."*
>
> — Sharon Lewis, director of *Brown Girl Begins*

A still captured from the Afrofuturist movie *Brown Girl Begins*.

A-HA! Moment 5

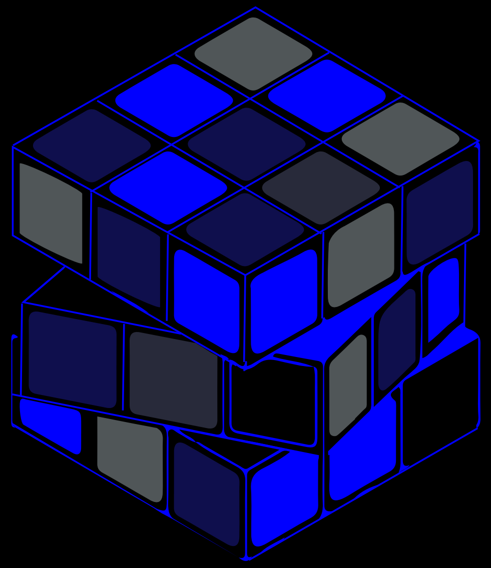
THERE ARE LOTS OF USE CASES FOR VISUALS

Visuals will be used by different people and for different reasons in the space. This can include toolkits for educational presentations or workshops, presentation decks aimed at decision makers, images in news articles or publications, public information or advocacy campaigns, advertising, workforce development marketing materials, and more.

A-HA! Moment 6

GROUNDING VISUALS IN REALITY EXPANDS UNDERSTANDING

Big things are happening in cyber and no one knows about it (because they can't see it). If we base our visuals on real events that are happening in our world, we can expand the capacity of the public to realize that the power of cybersecurity stretches beyond stealing credit card information. The Stuxnet worm impacted global affairs, yet the general public never internalized it — many don't even remember it. "When I talk about the 'Olympic Games' [the U.S.-Israeli operation that used the Stuxnet worm, well known in the cybersecurity space], they think I'm talking about sports," one expert said.



If someone flew to the U.S. and blew up a warehouse with a number of computers, leaders would be forced to respond in kind. If an attack of similar caliber occurs in the cyber world, experts say there is less of a response because it's not as tangible or accessible. This report is not advocating for more places being "blown up," and we're not looking for blind optimism. Instead, we aim to push for a higher level of understanding from all stakeholders so that informed decisions can happen.

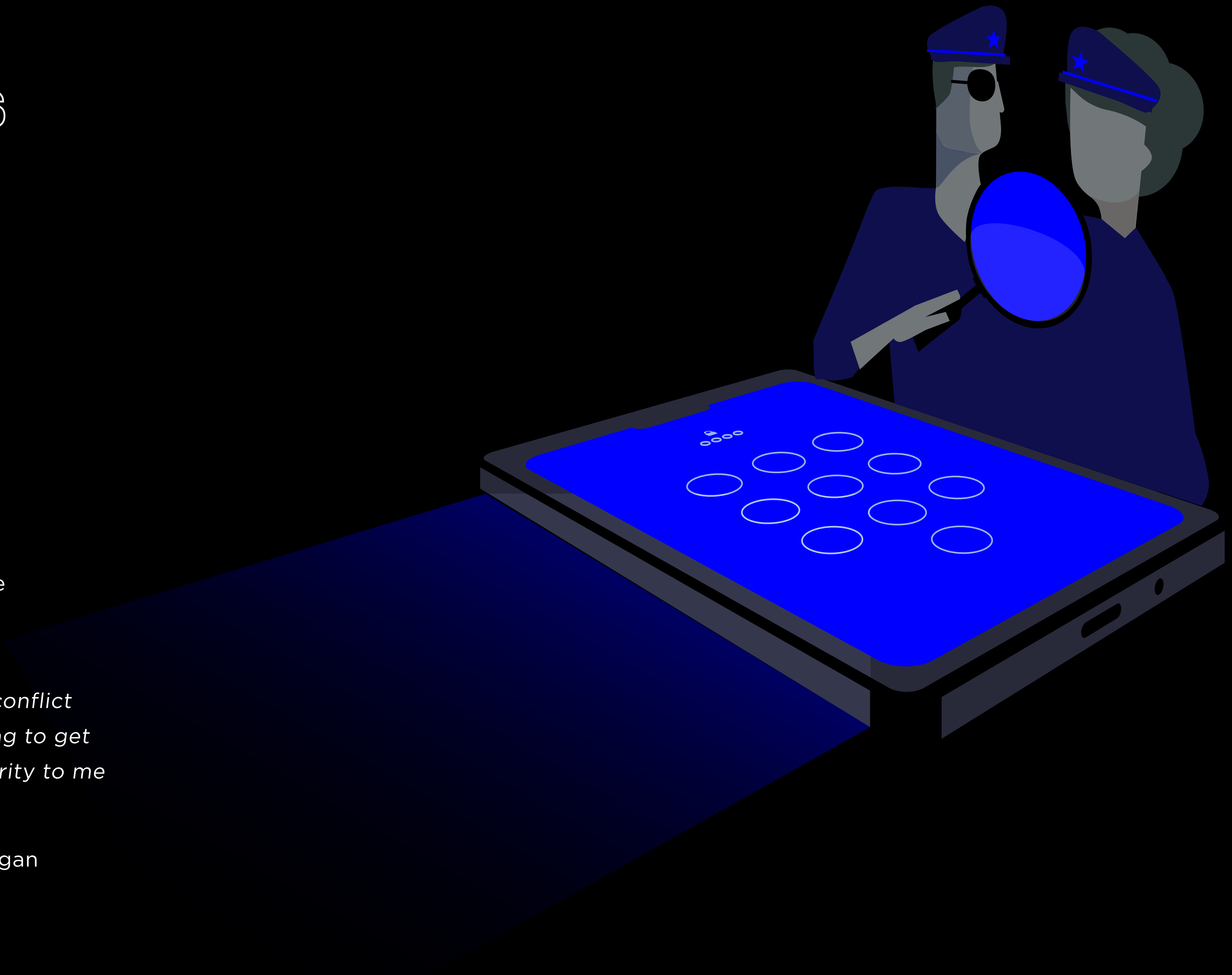
> *"What's surprising is the number of people who don't have a concept of the power of cyber beyond stealing credit card information."*
>
> — David Sanger, national security correspondent, *The New York Times*

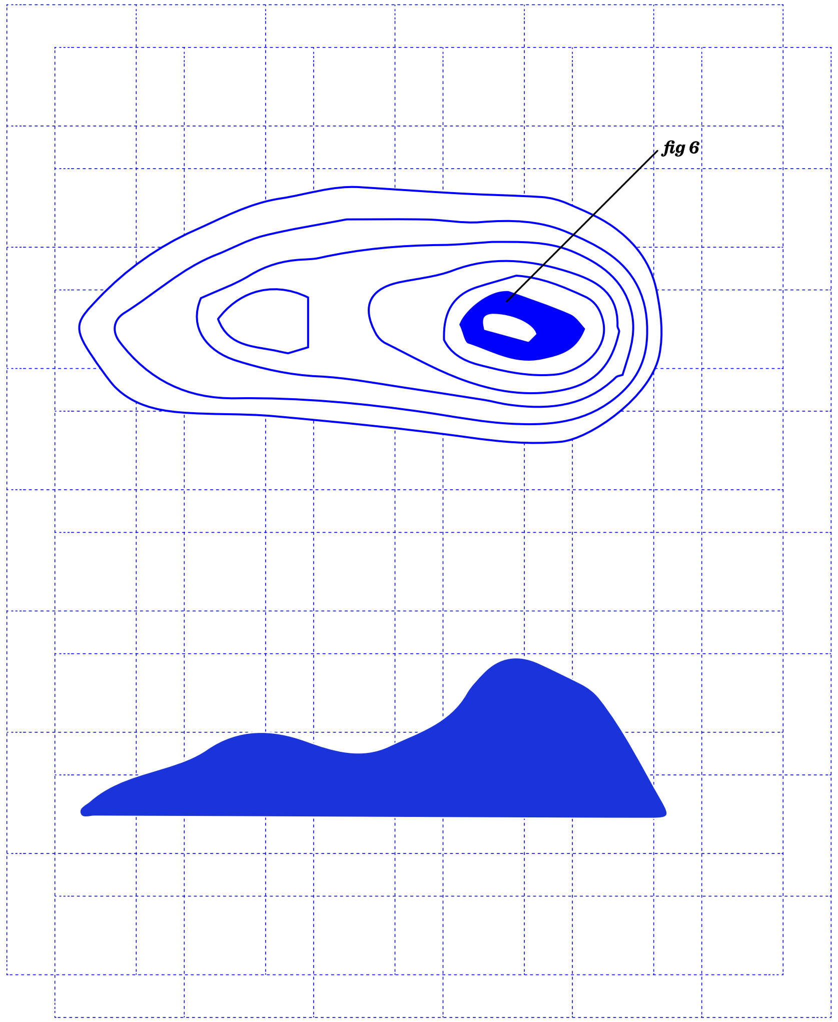
A-HA! Moment 7

IT'S ALL ABOUT THE TRADE-OFFS

All too often cybersecurity is depicted as a simple choice between an easy, perfect solution and an earth-shattering bad alternative. Reality is much more complicated. Many of the key cyber debates — ranging from encryption to combatting disinformation — involve hard trade-offs between our core democratic values: individual privacy and expression, personal and public security, and commerce and innovation. Visuals don't have to show the "right" answer to any of these debates. The mere act of depicting the trade-offs so people become aware of them is a critical first step.

> *"In a business, people who are the most in conflict with security efforts are those who are trying to get something good out the door, quickly. Security to me is a special case of quality."*
>
> — Ray Davidson, program manager at Michigan Cyber Civilian Corps





Chapter 6

TOOLS

During group sessions and interviews, we saw higher levels of engagement and insight when participants were able to actively interact with the content and draw their own conclusions and insights. To that end, we have included two tools in this report that can aid in understanding and exploring existing visuals in the space, and structuring and capturing feedback as you begin the design process.

VISUAL CANVAS

We bring a lot of assumptions with us as we design and it’s important to test these assumptions and interpretations, especially in a field with such high stakes. This visual canvas can help guide you through the feedback collection process and identify inaccuracies, alternate interpretations, and pitfalls of visuals.

VISUAL

Draw Your Cybersecurity Visual

What does this visual represent?

What are three emotions that this visual should evoke?

FEEDBACK

From a “Lay Person”

What does this visual represent?

What are three emotions that this visual evokes?

From another “lay person”

What does this visual represent?

What are three emotions that this visual evokes?

From a Technical Expert

What does this visual represent?

What are three emotions that this visual evokes?

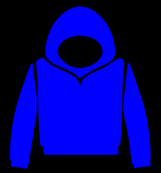
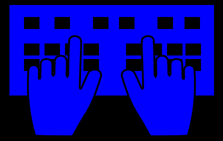
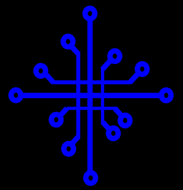
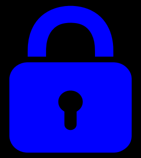
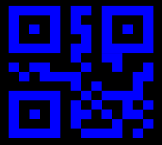
Is this visual accurate, technically?

Would you use it? When and how?

Are there any limitations to this visual or caveats with how it should be presented?

VISUAL CLICHÉS

This initiative is based on the fact that the visuals used in cybersecurity today do not fit the needs of the field. But don't just take our word for it: Take a moment to understand the visual clichés seen in cybersecurity today, and what may or may not be working about them.

VISUAL CLICHÉS	What are the emotions this image evokes?	Who do you think is the intended audience for this image?	What is this image trying to communicate?
			
			
			
			
			

WHAT'S AHEAD

There's so much opportunity for design to impact the cybersecurity space. As we aim to actively shape an optimistic, inclusive, and accessible field, we'll need collaboration between cybersecurity experts and visual creators, creative/brand directors for the space, universally recognized symbols, imagery that represents the actual humans behind cybersecurity, and visuals for specific terms and issues.

As we move forward, we hope to create space for visual creators to gain context and competency in cybersecurity, inspire subject matter experts to see the possibility of visual creations, and begin to craft the visual direction and assets that can move us toward a world where cybersecurity decision makers feel more prepared and empowered to create the policies and stories we need. We hope you join us.

AFTERWORD FROM THE HEWLETT FOUNDATION

Cybersecurity is a complicated challenge. Not just technically, but also on a policy level, because it involves thinking about how to make trade-offs among some of our most deeply held values: How do we balance privacy, security, and convenience, or choose between commercial innovation and regulation designed to keep us safe, to name just a few. And cyber policy is being made in a rapidly changing technical and social context, where the people who understand the technology best and the people charged with setting policy don't always see eye-to-eye, or even speak the same language.

These are some of the challenges the Hewlett Foundation's Cyber Initiative is working to address. And developing a new visual language for cybersecurity that begins to capture some of that complexity, and explain it to a wider audience, is one way to start bridging those divides. We're grateful to our colleagues at OpenIDEO and all the people who generously lent us their time and expertise to create this report. It's a great start, and it points to questions we still have about the way forward:

#1 How do we bring designers into a productive conversation with experts?

One reason the current state of cyber visuals is so bad is designers don't have access to the experts who could explain how to do it better. And experts don't often understand the craft of designers, or how to balance nuance and accuracy with accessible and engaging visuals. There's so much complexity in this topic, getting designers and experts talking to each other is critical for improving visuals, elevating the field, and expanding broad understanding of one of the most pressing issues we face.

#2 Do visuals need to have a strong point of view?

The Cyber Initiative is interested in building a broad, diverse field of cyber policy experts, and we often don't take a position on the debates within that field — our goal is to see experts with a variety of viewpoints engage with each other to inform policy debates. But can visual creators avoid taking a position, or does doing their best work mean having a point of view on the topics they're addressing? If the latter, we need a broad array of visual depictions that capture different views of the trade-offs that underlie key cyber policy debates. Otherwise, we risk a debate that is neither comprehensive nor inclusive.

#3 How can visuals remain durable?

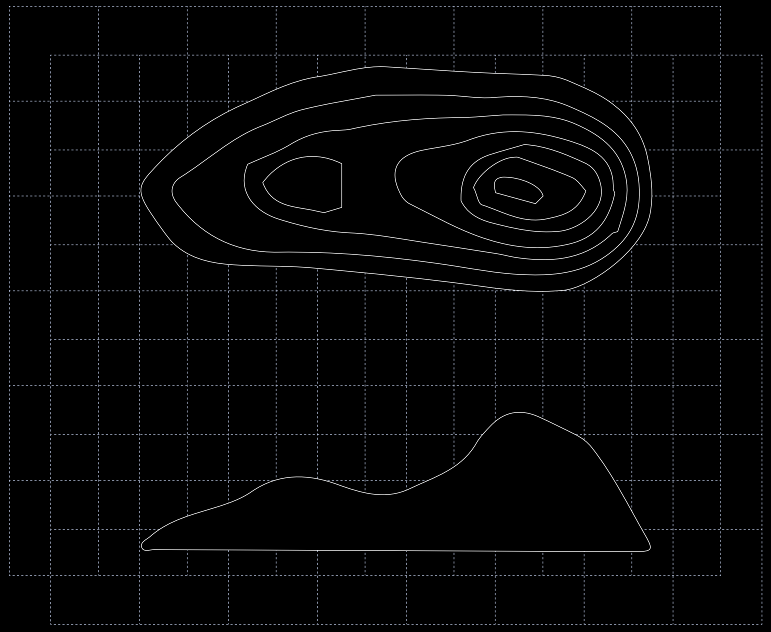
Given the rapid and constantly changing nature of this field, how can we keep up? What is the best way to develop a new and accurate visual language for cybersecurity, which captures some of its inherent complexities, while the field itself evolves? How can these depictions remain relevant and usable next year or the year after? Our hope is to support the development of depictions that could be further built on and evolve with time, but that also create an enduring visual map that makes cybersecurity more intelligible.

#4 What's the right visual approach?

During this research process, we saw visual creators begin to tackle this challenge using illustration, comic strips, collages, and infographics, to name just a few approaches. Their work incorporated humor, wonder, curiosity, friendliness, fear, and a whole range of very human personalities and emotions. Which will work best for increasing understanding of cybersecurity issues? And which approach will work best with which audience (e.g., policymakers in government vs. corporate boards, etc.)?

We can't wait to find out.

Eli Sugarman, Monica Ruiz, Heath Wickline



THANKS TO ALL OF THOSE WHO HELPED

This report would not have been done without the incredible support from a talented community of people around the world. Special thanks to the Hewlett Foundation (Monica M. Ruiz, Heath Wickline, and Eli Sugarman) who provided their expertise throughout the project. We also want to give our deepest gratitude to everyone who provided their wisdom and knowledge.

OpenIDEO/IDEO
Alex Nana-Sinkam
Caroline Moriarty
Erika Diaz Gomez
Hannah Lennett
Karen Lee
Njoki Gitahi
Scott Shigeoka

Hewlett Foundation
Eli Sugarman
Heath Wickline
Monica M. Ruiz

Individual Interview Participants
Andrew Grotto
Beau Woods
David Sanger
Elizabeth Weingarten
Eric Sears
Jeff Greene
Laura Bate
Ryan Evans
Ray Davidson
Ryan Calo
Sharon Lewis
Stephen Hiltner

Cybersecurity Experts
Andreas Kuehn
Ari Schwartz
Ashwin Mathew
Eva Galperin
Mike McNerney
Geoff Belknap
Heather King
Jessica Wilkerson
Joshua Corman
Kate Charlet
Leigh Honeywell
Leonard Bailey
Megan Reiss
Michael Hsieh
Michael Martelle
Paul Rosenzweig
Quinta Jurecic

Visual Creators
Abigail Kangogo
Arnold Young
Chela Cherwon
Diego Marini
Eric Moed
Gabrielle Kash
Gloria Chang
Jasmine Wilson
Jensine Eckwall
Joan Encarnacion
Kelsey Wroten
Leif Parsons
Matthew Willet
Ramya Anantharaman
Sarah Surrette
Tiff Hockin
You Jung Byun