



A Visual

FUTURE

of Cybersecurity

OPTIV

Life
imitates
art far
more
than art
imitates
life.

—Oscar Wilde

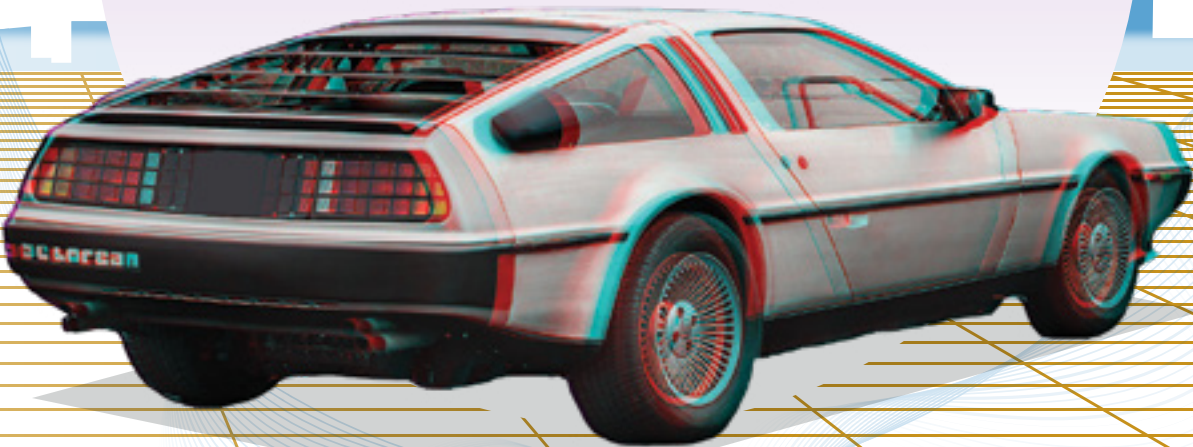
Current Reality or Science Fiction?

- ☐ An AI-driven drone kills enemy combatants without human intervention.
Current reality.
- ☐ A senior political leader fears enemies might assassinate him by hacking his pacemaker.
Current reality.
- ☐ A cartel establishes a venture capital fund to support innovation of new criminal technologies and practices.
Totally true
- ☐ Nation-states successfully hack the elections of rival nations.
Maybe too real.
- ☐ People have defibrillators embedded in their bodies. Hackers can take control of these devices.
This is real.
- ☐ A brain implant allows people to control computers with their minds.
Also real too.
- ☐ Hackers dupe a company out of a huge sum of money by replicating its CEO's voice with a computer.
100% true.
- ☐ Urban residents and visitors can hail an autonomous flying taxi.
Really very true.
- ☐ A large audience watches as a security researcher hacks an insulin pump.
Oh so true.
- ☐ Artificial intelligence replaces journalists and marketing writers.
Current reality.
- ☐ Taking a cue from legitimate business, hackers market crime "as-a-service" offerings.
Totally true.
- ☐ A quantum computer decrypts a previously uncrackable encryption in a few hours.
Terrifyingly true.
- ☐ Consumers purchase internet-connected condoms.
Truly truly true.
- ☐ A research team creates a type of matter that ignores Newton's second law.
True.

The Future is So ... Yesterday

The problem with writing about the future is that something you're speculating on might actually happen before you get the book on the shelves. This is a particular hazard when your world is essentially science fiction already.

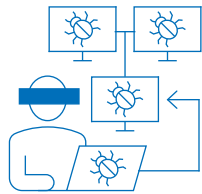
So our notion of "the future" is...fluid. We've already rewritten multiple sections because the pace of innovation overran us, and we hope you'll forgive us if tomorrow is yesterday's news by the time you read this.



Answer: All are either current reality or will be possible in the very near future.

Lately we find ourselves reflecting on

cy·ber·punk 1) science fiction dealing with future urban societies dominated by computer technology; 2) an opportunistic computer hacker.



Literature

Cyberpunk emerged in the 1980s, building on the writing of William Gibson, Bruce Sterling and, later, Neal Stephenson. The dystopian, noir science fiction (SF) subgenre drew on and expanded the gritty visions of SF New Wavers like Philip K. Dick and Roger Zelazny.



Movies and TV

If you watched "The Matrix," you've been exposed to cyberpunk. Ditto "Mr. Robot," "Black Mirror," "Blade Runner" (the original and "2049"), "Total Recall," "Ready Player One," "Westworld," "Max Headroom," "Almost Human," "Altered Carbon" and "RoboCop" (as well as a couple of "X-Files" episodes). If you want to get a tad more exotic, the classic Japanese anime (and 2017 Hollywood adaptation) "Ghost in the Shell" is as cyberpunk as it gets.



Music and Other Mediums

Nine Inch Nails, Madonna, David Bowie, Janelle Mon  e, Daft Punk, Grimes and Rob Zombie draw on cyberpunk themes, and the gaming world is making a fortune on the genre with titles and franchises like "Halo 3 ODST," "Call of Duty," "Shadowrun," "Deus X," "System Shock" and, of course, "Cyberpunk 2077."



Typical elements of cyberpunk include:

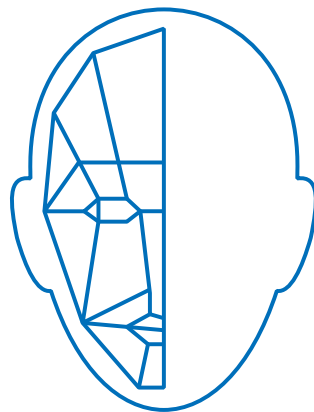


SkyNet vs. SkyNot



Why are we talking about science fiction?

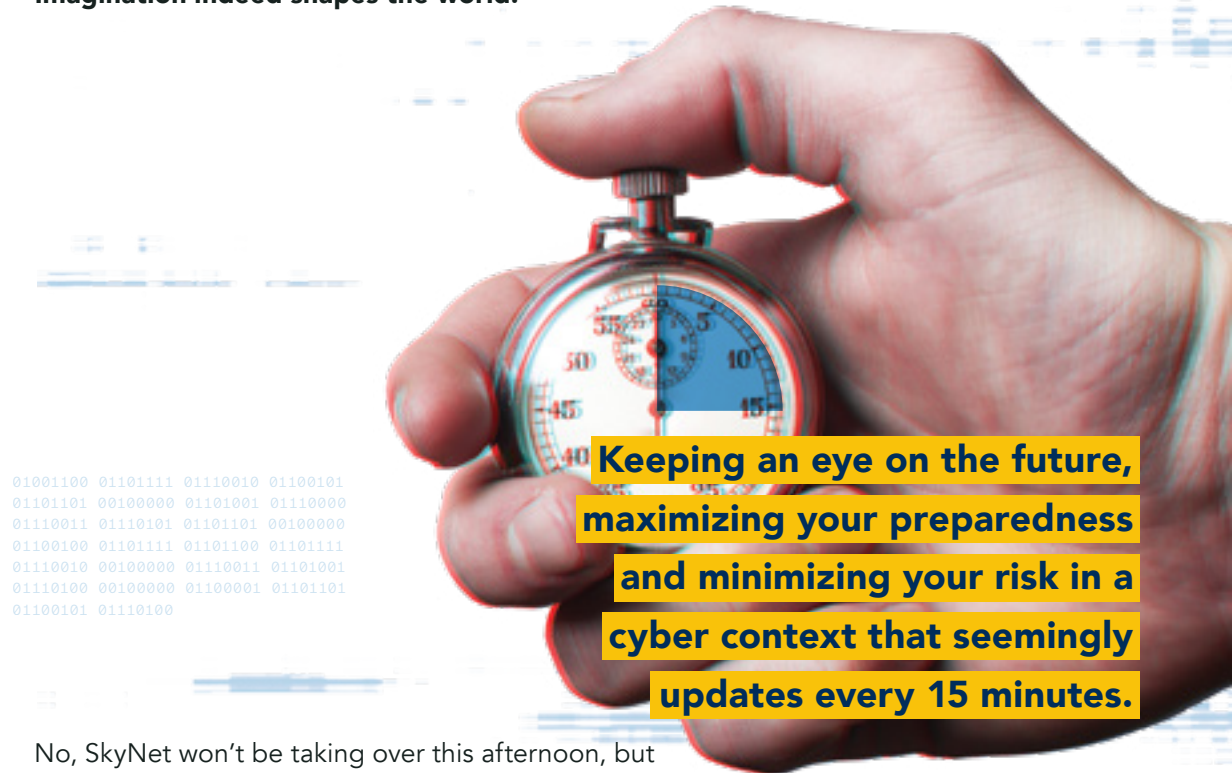
Because, as we explained in a 2020 blog,¹ if you want to know what the world will look like tomorrow, study the SF of today. Sci/tech development historically takes its cues from fiction and film. Moreover, **it does so deliberately and the pace is accelerating.**



In the introduction to **AI 2041**,² co-author Chen Qiufan, formerly a Silicon Valley technologist, puts it more elegantly.

“A lot of people would assume engineers and computer science wizards might have little interest in fiction... But during my more than ten years working in tech, I encountered many engineers and technologists who were not-so-secret fans of speculative fiction... From the modern submarine to the laser gun, and from mobile phones to CRISPR, scientists will readily admit they got direct inspirations from fiction.

Imagination indeed shapes the world.”



Keeping an eye on the future, maximizing your preparedness and minimizing your risk in a cyber context that seemingly updates every 15 minutes.

No, SkyNet won't be taking over this afternoon, but Gibson's depiction in "Neuromancer" of hackers and nation-state military cybercrime was uncomfortably prescient. So while Optiv is deeply invested in safeguarding your operations and helping you develop strategy that accounts for the cyber threats you face each day (as well as the profound opportunities represented by digital transformation innovations), we feel an obligation to keep an eye on the future, maximizing preparedness and minimizing risk in a cyber context that seemingly updates every 15 minutes.

Table of Contents

This e-book considers five significant emerging/
future trends in cybersecurity:

[artificial intelligence\(pg11\)](#)

[quantum computing\(pg29\)](#)

[ransomware\(pg49\)](#)

[the ubiquitous attack surface\(pg59\)](#)

[evolving cyber criminal business](#)

[models\(pg83\)](#)



Click to jump
to a chapter

We explain where we are, where we're heading and what the implications are for your organization. The cybersecurity industry, especially, demands effective thought leadership that pays close attention to the places where the future is closing on us quickly – or has already arrived. We hope this book prompts some reflection by you and your team, and we look forward to discussing your future.

Your Mileage May Vary

Predictions about when **x** will happen vary widely (especially when the topic is powerfully transformative tech like artificial intelligence or quantum computing). Some sources (often, it must be said, people with financial interest in a potential product) argue that **x** will be technically or commercially viable sooner rather than later. Others, such as Kai-Fu Lee and Chen Qiufan (authors of “AI 2041”), foresee a longer timeline (in this case, a 20-years-out horizon). And a few, like Amy Webb (author of “The Big Nine”), take a far more conservative (as in, 50–100 years) view.

These predictions diverge for any number of reasons, including a wide range of assumptions about the pace of progress and the basic difficulty of knowing the future (because technology is hard). When we reflect on tech development in recent decades, it seems like “just around the corner” predictions often take longer than expected, while things we believe are decades out happen a lot sooner than expected. So your mileage may vary...

A Note
About
Timelines



Artificial Intelligence

"AI will probably most likely lead to the end of the world, but in the meantime, there'll be great companies."

—Sam Altman
Chairman, OpenAI

01100001 01110010 01110100 01101001
01100110 01101001 01100011 01101001
01100001 01101100 01100000 01101001
01101110 01110100 01100101 01101100
01101100 01101001 01100111 01100101
01101110 01100011 01100101

01100001 01110010 01101100 01101001 01100110 01101001 01100011 01101001 01100001 01101100
00100000 01101001 01101110 01101100 01100101 01101100 01101100 01101001 01100111 01100101
01101110 01100011 01100101

“AI is one of the essential pillars for any company with aspirations to grow into the next generation.”



Dave DeWalt
Founder and Managing
Director at NightDragon

What's Driving Artificial Intelligence?



Organizations are Getting the Message

McKinsey's State of AI report in 2020 found that **58% of respondents** have adopted artificial intelligence in at least one phase of their business⁴;

...another analysis forecasts **total global AI spending to top \$190 billion by 2025** (up from \$21.46 billion in 2018).

Most Popular AI and Machine Learning Applications

Data Analytics

Threat Hunting

Risk Scoring

Behavioral Analysis

Vulnerability Management

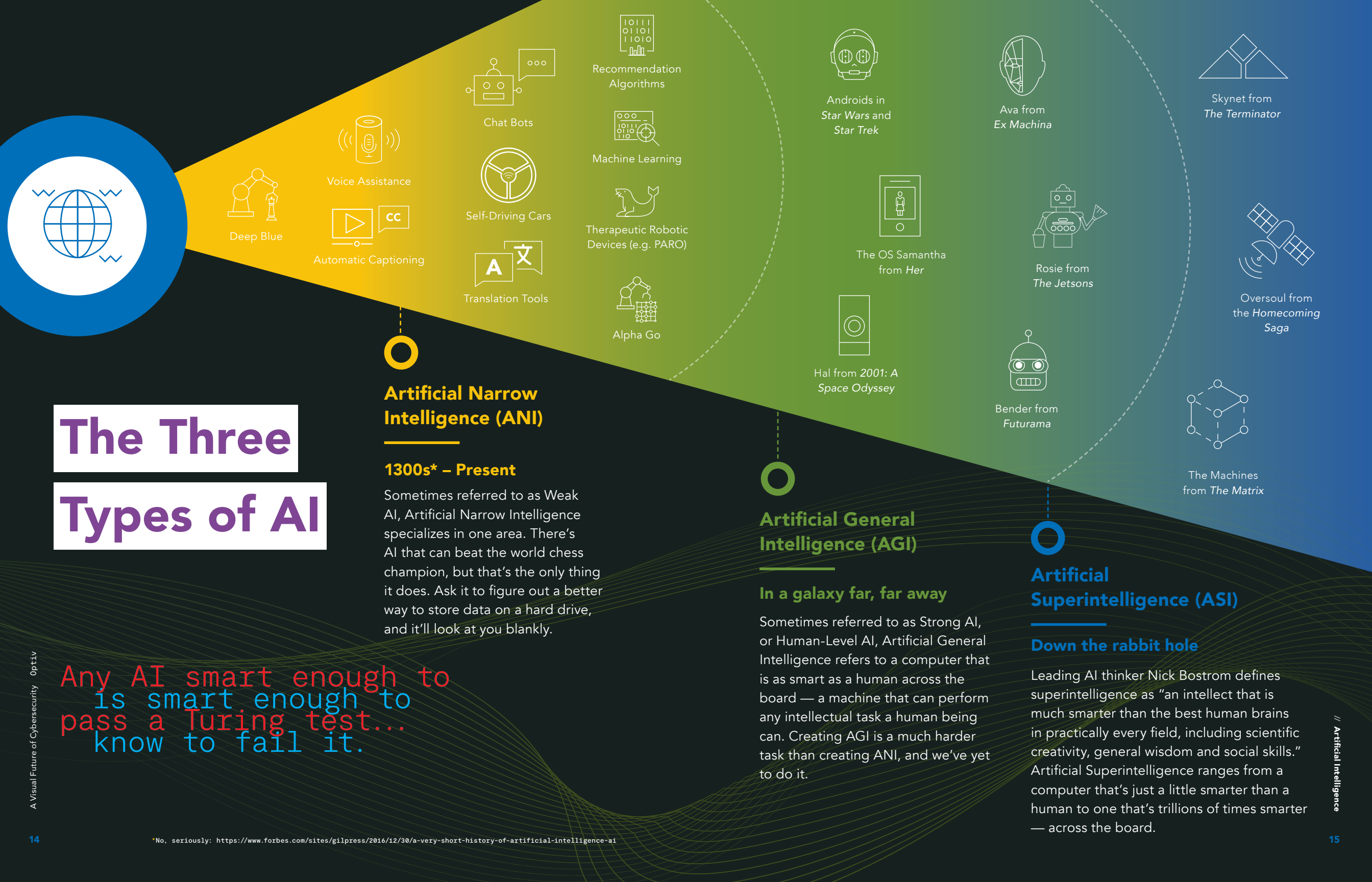
AI+ML

In addition to the sheer power represented by AI technologies, organizations will also be motivated by their speed and cost (as well as their ability to help mitigate the industry's critical talent shortage).

By the Year 2040

AI applications, in combination with other technologies, will benefit almost every aspect of life, including improved healthcare, safer and more efficient transportation, personalized education, improved software for everyday tasks, and increased agricultural crop yields.⁶





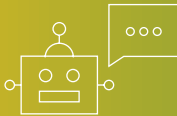
Deep Blue



Voice Assistance



Automatic Captioning



Chat Bots



Self-Driving Cars



Translation Tools



Recommendation Algorithms



Machine Learning



Therapeutic Robotic Devices (e.g. PARO)



Alpha Go



Androids in
Star Wars and
Star Trek



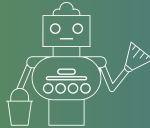
Ava from
Ex Machina



Skynet from
The Terminator



The OS Samantha
from *Her*



Rosie from
The Jetsons



Hal from 2001: A
Space Odyssey



Bender from
Futurama



Oversoul from
the *Homecoming*
Saga



The Machines
from *The Matrix*

The Three Types of AI

Artificial Narrow Intelligence (ANI)

1300s* – Present

Sometimes referred to as Weak AI, Artificial Narrow Intelligence specializes in one area. There's AI that can beat the world chess champion, but that's the only thing it does. Ask it to figure out a better way to store data on a hard drive, and it'll look at you blankly.

Any AI smart enough to
is smart enough to
pass a Turing test...
know to fail it.

Artificial General Intelligence (AGI)

In a galaxy far, far away

Sometimes referred to as Strong AI, or Human-Level AI, Artificial General Intelligence refers to a computer that is as smart as a human across the board — a machine that can perform any intellectual task a human being can. Creating AGI is a much harder task than creating ANI, and we've yet to do it.

Artificial Superintelligence (ASI)

Down the rabbit hole

Leading AI thinker Nick Bostrom defines superintelligence as "an intellect that is much smarter than the best human brains in practically every field, including scientific creativity, general wisdom and social skills." Artificial Superintelligence ranges from a computer that's just a little smarter than a human to one that's trillions of times smarter — across the board.

*No, seriously: <https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai>

AI and Machine Learning (ML) technologies are already useful for some important cyber defense tasks.

Near-future developments will produce better predictive analysis, as AI defenses onboard more data about existing and emerging attacks, factoring it into their capabilities.

AI

The goal of AI is to make a smart computer system like humans to solve complex problems.

In AI, we make intelligent systems to perform any task like a human.

AI is working to create an intelligent system which can perform various complex tasks.

ML

The goal of ML is to allow machines to learn from data so that they can give accurate output.

In ML, we teach machines with data to perform a particular task and give an accurate result.


Machine learning is working to create machines that can perform only those specific tasks for which they are trained.

ML is very good at sifting through massive amounts of data and detecting patterns and anomalous behavior – a major boon for any large enterprise and many mid-market businesses. It's also adept at understanding individual user behavior. Once a set pattern is established, deviations may indicate a user account was hacked or that there may be an insider threat concern.


What About AI as an Attack Tool?

Hackers are already exploring applications for AI (weaponizing malware, countering cybersecurity advances, etc.)⁷.


Specific uses include:




Concealing malicious code




Triggering/executing attacks




Modeling and developing more adaptable attack techniques



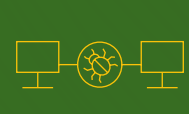
Blurring the line between real and make-believe



Creating intelligent malware



Executing intelligent, self-propagating attacks



Creating malware capable of mimicking trusted system components

“ They program the codes to execute at a specific time, say ten months after the applications have been installed, or when a targeted number of users have subscribed to the applications. This is to maximize the impacts such attacks will cause. Concealing such codes and information requires the application of AI models and deriving private keys to control the place and time the malware will execute.” — **Julien Legrand** Société Générale⁸

Hackers are also incorporating AI-driven tools to “finalize malware payloads before use⁹, similar to the sophisticated encoders, packers and obfuscators used today. Researchers have demonstrated proof-of-concept (POC) tools that can be used to defeat even the most advanced AV systems.”

Also, just as blue teams can use AI to crunch massive volumes of data in search of tell-tale attack patterns, hackers will likely be able to use the same analysis-at-speed capabilities to efficiently identify better targets (as well as drive improved automation). We also envision AI attacks adapting on the fly to evade detection based on controls encountered.

“AI is going to be extremely beneficial, and already is, to the field of cybersecurity. It’s also going to be beneficial to criminals.”

— **Dmitri Alperovitch**
Co-founder, Former CTO, CrowdStrike



AI/ML: Hacking, Poisoning, Bias

Artificial intelligence already runs huge chunks of the modern world. Adoption is widespread because AI is easy to use. Sure, creating new AI models requires significant computing resources and expertise, but trained models are easily deployed into micro-computers, connected devices and cloud services. And laptops, refrigerators, websites and cars...

Since many AI models are publicly available, and resourceful hackers can find the research papers, datasets and code used to develop them, the bad guys can now plot new attacks and slip past existing cybersecurity frameworks. Further, when AI models are widely used, exploits that work against one target can be quickly adapted for any organization using the same models.

Every business will benefit from AI. But not every business will employ a team of data scientists and researchers. Open-source and vendor-provided models will continue to proliferate. These resources lower costs and increase ease of use, but they also introduce novel vulnerabilities.

AI/ML Poisoning

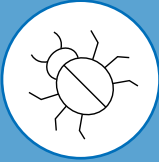
Machine learning poisoning is the malicious introduction of bad data into the algorithm's training data with the intent to corrupt or weaken it.

"It seems hyperbolic to call it a battle between good and evil, but lives, careers, families, businesses and the well-being of society generally are very much on the line. So even if you feel we're being dramatic, there's no denying just how much is at stake."

—Randy Lariar
Director Big Data & Analytics, Cyber Digital Transformation, Optiv



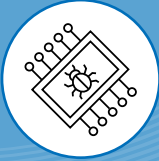
ML poisoning attacks target (and thrive) on humongous datasets that are too big for humans to process. Even subtle alterations can skew outcomes in potentially catastrophic ways.



Microsoft launched the Tay chatbot for children's entertainment in 2016. Within 16 hours, hackers attacked the bot, feeding it adversarial data and fueling a stream of racist and sexist posts to its Twitter feed.¹⁰ The highly public debacle drew intense scrutiny and made clear that AI models are uniquely vulnerable.



Some AI/ML poisoners are more comfortable in the shadows, though, quietly altering training data so they can hijack the model later. For instance, researchers have corrupted autonomous car data to fool vehicles when they detect a particular symbol. Imagine approaching a railroad crossing when the onboard camera sees a sticker on the warning sign and, instead of braking, it accelerates.





Now, for fun, imagine that the poisoning happens at the operating system level and a whole product line is affected... but no one knows it until it triggers.






Hackers are already exploring applications for AI (weaponizing malware, countering cybersecurity advances, etc.).⁷



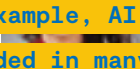
Bias




AI models don't manifest prejudice by default, but the data and processes used to train them can unintentionally teach them bias¹¹. Datasets inherently reflect the racial/ethnic, gender, religious, cultural, socio-economic and nationality assumptions of the cultures developing them. Unmonitored, AI will also mirror the subtle, unobserved biases of the context in which it's collected.




 I'm not a robot 



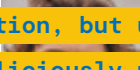
Select who you think is the **Chief Information Security Officer?**











1

Verify

For example, AI is already embedded in many HR and staffing processes. These groups champion diversity and inclusion in hiring and promotion, but unintentional or maliciously planted bias can occur.

What, for instance, does the phrase "cultural fit" mean? How might the unarticulated biases it represents worm their way into AI training?

Consider a company in which minorities and women are underrepresented. As it works to recruit and retain people who match its "top performers" profile, it might inadvertently teach its AI-driven applicant tracking system the wrong lesson.

What constitutes a successful employee at this company?

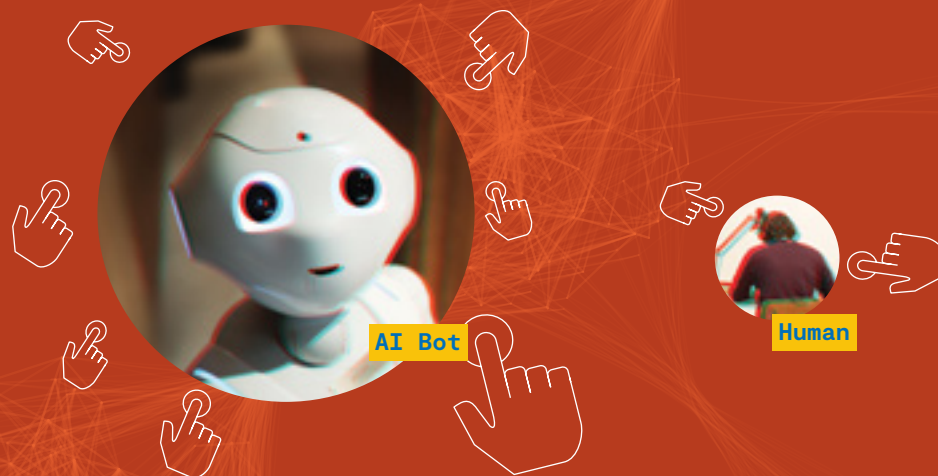
Might it overemphasize white and male because that's what most employees currently are? Does the AI accidentally come to favor upper middle-class language patterns in résumés in ways that dismiss qualified working-class applicants?

There are already many studies and technical approaches to detect and mitigate bias in AI models, but they assume good intent. Even if the good guys get it right, the bad guys have an interest in manipulating AI models. Future cybersecurity and AI governance will grapple with all of these issues.

Artificial Faking

In addition to executing attacks, artificial intelligence will prove incredibly useful in their construction and innovation.

AI will be a bonanza for social engineering. If you've ever received a phishing email (we're guessing you have) you know one of the tipoffs is how poorly written they typically are. But what if the email is written as well as — or better than — a real person?



At Black Hat 2021 a Singapore government agency sent phishing emails they crafted as well as others generated by an AI as-a-Service platform to 200 colleagues.

Surprisingly, a significant margin of people clicked the links in AI-generated messages compared to the human-generated ones.

Welcome to OpenAI's GPT-3, a platform that generates text that's difficult to distinguish from that of real human authors — **today**.

Before GPT3

To: Alex Smith
From: customercare21@abc.co.net
Dear customeer,
Youre password has expired.
Please reset by 11pm pst, to
avoid being locked out of your
account.

If your account is locked
12 hours you're account is
suspended.

Thanks,
abc customer Care

To: Alex Smith

From: Susan Meyer

Hi Alex!

I accidentally got logged out of
our ABC team account. Says they
just sent you a authentication
code. Could you please send on to
me so I can verify the account to
log back in?

Thank you!

Susan M, Sr. Legal Analyst

Send @ | +

After GPT3

Seeing Will Not Be Believing

Expect emerging deepfake technology to take the deception to the next level.



Add rapidly improving video capabilities to the mix — you may have seen “The Shining” videos where Jim Carrey deepfakes Jack Nicholson or the more recent Tom Cruise videos — and the potential for mayhem is alarming. Just for fun, go Google “deepfake videos” and spend a few minutes watching.

There is no realm of cybercrime where deepfakes don’t pose a significant threat



Spear-phishing



Political and hacktivism

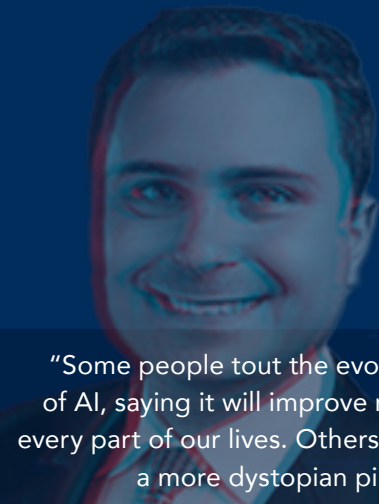


Extortion of individuals and organizations

Potential applications for the technology go on and on.

2018 saw deepfakes enter the public’s consciousness when comedian/director Jordan Peele used AI techniques to create a deep fake video of former President Obama speaking to the dangers of fake news.

(See the Ransomware chapter later for more fun with deepfakes.)

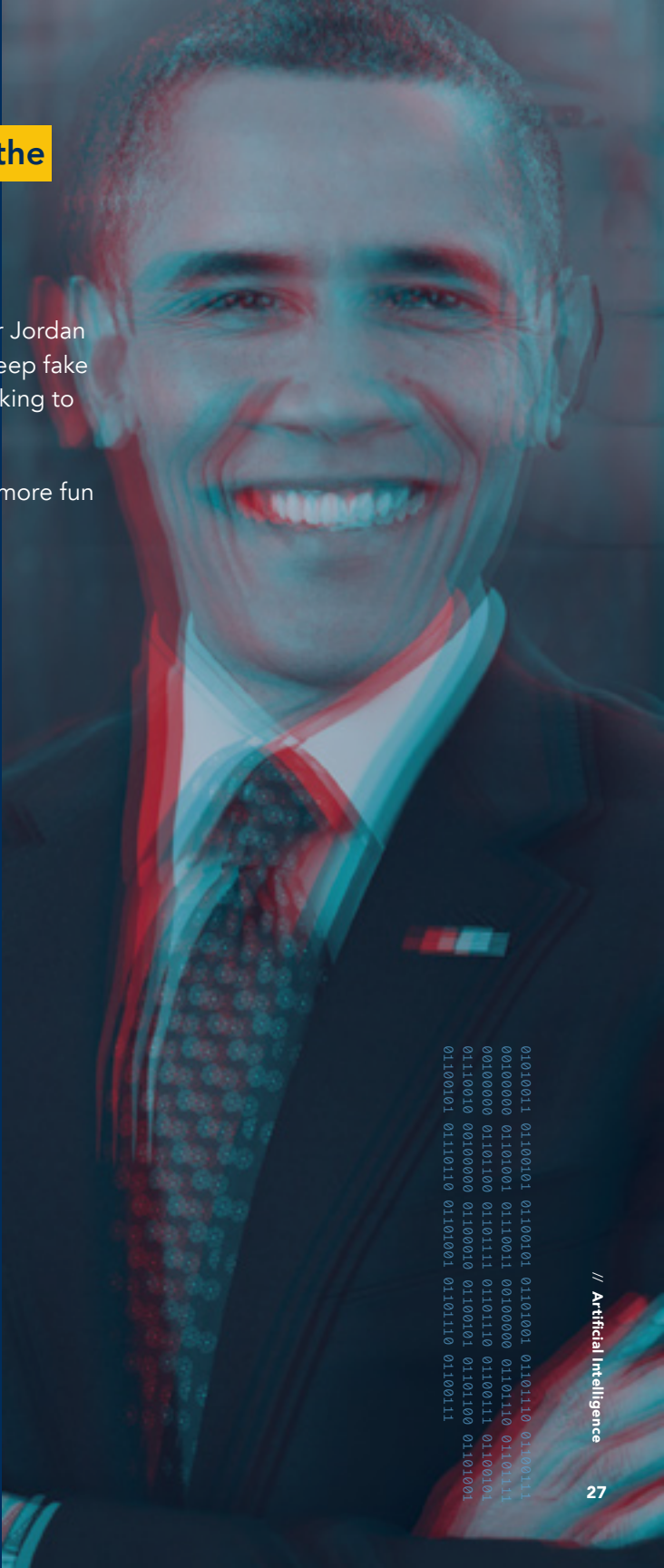


“Some people tout the evolution of AI, saying it will improve nearly every part of our lives. Others paint a more dystopian picture.

So which is it? History tells us it’s both/and, not either/or. It’s up to us to implement innovation so that it drives the greatest benefit for the most people, while minimizing harm to people’s lives and livelihoods. There’s much to be hopeful about if we get it right, and plenty to be concerned about if we don’t.”

—Randy Lariar

Director Big Data & Analytics,
Cyber Digital Transformation,
Optiv



01101001 01100101 01100101 01101001 01101110 01100111
00100000 01101001 01100111 00100000 01101111 01101111
00100000 01101100 01101111 01101110 01100101 01100101
01100100 00100000 01100010 01100101 01101100 01101001
01100101 01101010 01100101 01101110 01100111

"A classical computation is like a solo voice — one line of pure tones succeeding each other. A quantum computation is like a symphony — many lines of tones interfering with one another."
— Seth Lloyd



Quantum Computing

01110001 01110101 01100001
01101110 01110100 01110101
01101101 00100000 01100011
01101111 01101101 01110000
01110101 01110100 01101001
01101110 01100111

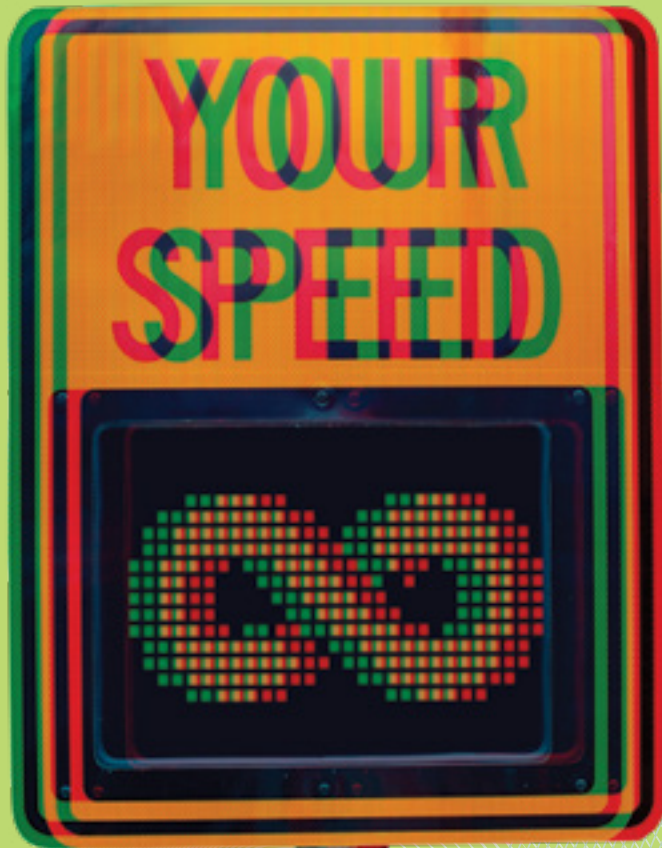
01110001 01110101 01100001 01101110 01110100
01110101 01101101 00100000 01100011 01101111
01101101 01110000 01110101 01110100 01101001
01101110 01100111

Quantum computing (QC) uses quantum theory principles to execute operations significantly faster than today's most powerful computers.

How Much Faster?

In 2019, Google claimed its experimental system **performed a calculation in 200 seconds that would take the world's most advanced supercomputer 10,000 years**. In 2020, a Chinese research team reported results 10 billion times faster than Google's.

Classical computers — including Fujitsu's Fugaku (the most powerful supercomputer in the world... for the moment), your laptop and everything in between — crunch bits (encoded as ones and zeros). **But quantum systems have a third state — "superposition" — that allows for one, zero and both. As such, two "qubits" can process four scenarios at once.**



Businesses need to be ready for a quantum future because it's coming.

Quantum Computing and Cybersecurity

J 6 0 q 9 3 6 r S M I K t A E 8 K g y m
d g y Z t 4 9 A Z r A C k h 5 5 M a L 4
W U M Y W n 6 D p d Y n X N f g 4 T Q 7
l w 8 N B M 4 W h a R L S c P Q B S 3 I
P B L Q 0 j e j N X b 0 4 0 c u k C P P
8 l m 9 h U 0 B U l o Z u 1 c 4 C 2 d A
v C n P a w H 7 h n h f e Q a i u l C v

In security, quantum computing's most obvious implications are for cryptography: what will be its impact on our ability to encrypt and safeguard data, networks and systems?

Some predict that QC will, within the next 20 years, be able to break any existing encryption system,¹⁶ which is... concerning.

Are these predictions true?
Yes and no. Kinda.

Encryption employs an algorithm-generated key based on a complex mathematical problem. It's theoretically possible to break any encryption so long as you have the power and time required to try every possible key. The time required, though, can run into thousands, even millions of years (literally) depending on the encryption used.

Modern cryptosystems like TLS often use strong symmetric algorithms such as the Advanced Encryption Standard (AES) from the National Institute of Standards and Technology (NIST) to encrypt data for secure transmission over the internet or other channels. Symmetric algorithms aren't especially vulnerable to advances in quantum computing. AES is built on a complex substitution-permutation network principle, and while a QC could crack AES-128 in around six months

Deciphering AES-256 encryption could take as long as

10.8 quintillion years

That's just 785 ages of the entire universe multiplied by a million...

So We're Safe?

Here's the hitch: while the Advanced Encryption Standard is quantum-resistant, the mechanisms currently used to exchange AES keys are threatened by QC. (You need the key to unlock the encrypted data – how do I get that to you securely?) Several public-key cryptography (PKC) systems (aka "asymmetric" cryptography, like Rivest-Sharmir-Adleman [RSA] and elliptical-curve [EC]), are frequently employed to secure the transmission of AES keys.

RSA is practically unbreakable by classical computers because of the vast amounts of time required. But a sufficiently powerful QC system could crack the most advanced RSA encryption in a few hours.¹⁸ RSA and EC are currently safe because the underlying mathematics required to crack them (large integer factorization, computing inverse logs, etc.) are difficult for modern computers to solve. QCs, on the other hand, are especially good at these computations.

In other words, AES is safe from QC, but an attacker who can crack the asymmetric crypto used for the key exchange can use the stolen key to decrypt the AES traffic. Without a way to securely communicate the key between two parties, the confidentiality of symmetric crypto can't be guaranteed.



Post-Quantum Cryptography

“Quantum-proof” refers to algorithms that can withstand attack by a quantum computer. NIST is currently working to adopt and establish a standardized post-QC encryption standard and expects to complete the process in 2022.¹⁹ It began with 69 candidates in 2017 and has now narrowed the field to seven finalists and eight alternates (including the “Classic McEliece,” touted as quantum-proof by MIT as early as 2010).²⁰

Between existing protocols like AES and a new full-on NIST standard in the not-too-distant future, then, the world seems relatively safe from malicious actors with quantum computers (assuming development of a QC-proof approach to replace RSA).

Almost...

Retrospective

Decryption

There’s another issue to consider. Nation-states and criminal organizations are stockpiling encrypted data to potentially decrypt when technology catches up. QC will be a huge catalyst for this, which is why we need to look forward now.

If an asset needs to be secret for 20 years then its encryption needs to anticipate the cracking capabilities available in the early 2040s.

ddoqUKaygXI
AGT1CL3zpXA==

2040

vp2rBiiYTB
Xq5ZwkVz4hrA==

2020

// Quantum Computing

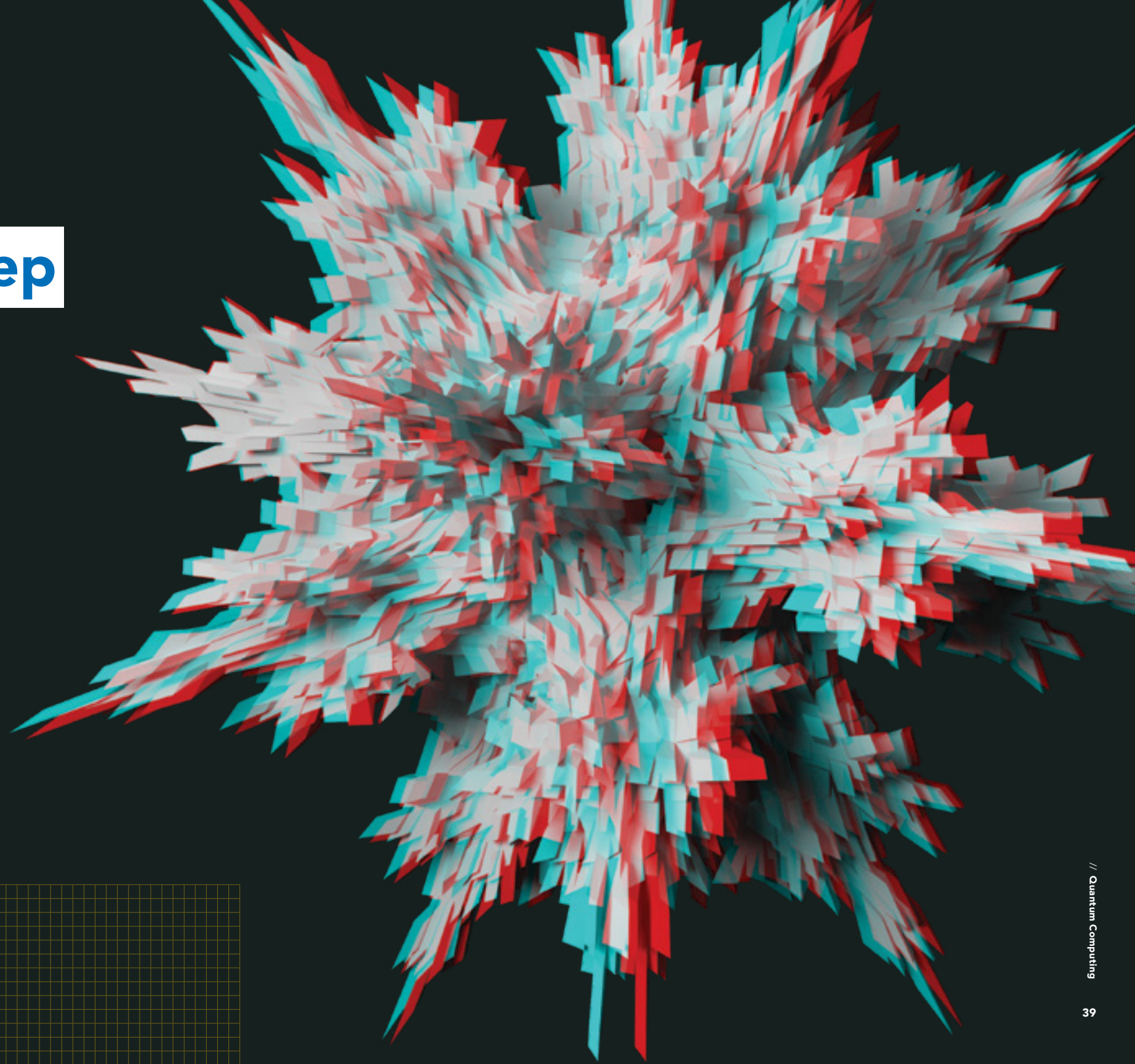
Are There Any What-Ifs to Keep an Eye On?

Of course, and they mainly revolve around “how soon?”

Most experts say QC won't be a threat to encryption in the near future – Lee and Qiufan estimate 10-30 years. A number of obstacles must be addressed:

It is estimated that a QC will likely need a million or more physical qubits in order to deliver the performance of a 4,000 logical qubit QC. And even when a useful quantum computer is successfully demonstrated, mass production is another matter.

Finally, quantum computers are programmed completely differently from classical computers, so new algorithms will need to be invented, and new software tools will need to be built.



Beyond That the Picture Gets Blurry

and some of the research being conducted threatens to rewrite all the rules.

For instance: a team featuring dozens of scientists from Stanford, Princeton, Columbia, MIT, the University of Chicago and other universities working with Google's quantum computing labs may have created the world's first time crystal inside a quantum computer.^{21 22}

Time crystals are like perpetual motion machines, "forever [cycling] between states without consuming energy." If they exist, they violate Newton's second law,²³ and in doing so represent an unprecedented source of stability for quantum computers.

Newton's Laws of Motion

#1 Inertia An object at rest remains at rest, and an object in motion remains in motion at constant speed and in a straight line unless acted on by an unbalanced force.

#2 Force The acceleration of an object depends on the mass of the object and the amount of force applied.

#3 Action & Reaction Whenever one object exerts a force on another object, the second object exerts an equal and opposite on the first.

TELE

PORTATION

Then there's AMD's patent application for "[l]ook-ahead teleportation²⁴ for reliable computation in multi-SIMD quantum processor."

It looks like the company is researching systems involving quantum teleportation processes. The aim is to improve the current reliability of quantum computing, and even reduce the number of qubits necessary to make accurate calculations.

Neither technology is going to be ready for prime time soon, but there's every reason to track mind-bending innovation. Once we can see that generation of quantum tech heading our way we'll need to rethink basically everything we think we know.

Finally,

One recent development could hit the radar sooner rather than later. Researchers at Japan's Riken Center for Emergent Matter Science "have demonstrated a triple-qubit, silicon-based quantum computing mechanism."²⁵

"Two-qubit operation is good enough to perform fundamental logical calculations. But a three-qubit system is the minimum unit for scaling up and implementing error correction," notes Seigo Tarucha, who led the team of Riken researchers.

Thanks to the breakthrough, Riken researchers think they can build a "large-scale quantum computer" within a decade.

We'll see.

Digital

Quantum

Transformation

Quantum systems will have tremendous applications for many (if not most or all) industries. For instance:

Healthcare

For starters, QC will dramatically reduce the time required to sequence a genome, enabling better predictive analysis. It can help diagnose patients more quickly and accurately, and it will also allow physicians to tailor treatments to specific individuals. On the business side, quantum systems can drive down costs and help optimize insurance premiums.

Pharma

QC is already used by biopharmaceutical companies in limited applications and is expected to dramatically transform the process of drug discovery and development.

Weather/Climate

QC's analytical power will substantially enhance forecasting, enabling highly localized reports. On the climate front, quantum advances will (as with pharma R&D) help researchers simulate large, complex molecules that can drive development of atomic structures that readily bind to carbon, allowing us to "suck" it out of the air.²⁷

Traffic

Traffic in large urban areas is one of our most complex real-world challenges, with significant implications for air quality and fuel use (to say nothing of the basic human costs associated with wasting dozens of hours a year in frustrating jams). Volkswagen has demonstrated that QC can power traffic management systems to help drivers identify the fastest routes to their destinations. Imagine this kind of tech integrated into all cars and applied to entire smart city grids.

Financial Services

Banking, insurance and investment businesses rely heavily — and increasingly — on the ability to crunch huge amounts of (often unstructured) data. Analysts see FS benefitting tremendously from QC, as it will help them better manage risk, predict outcomes and drive automated trading. Customers also benefit, as quantum-powered institutions will be able to make stronger portfolio recommendations.

Chemistry

The American Chemical Society believes chemistry will be QC's killer app.²⁸ It can boost "renewable chemical manufacturing, enable deeper understanding of the enzymes that underlie photosynthesis and the nitrogen cycle, power the discovery of high-temperature superconductors and new materials for solar cells, and much more."

Manufacturing and Materials Science

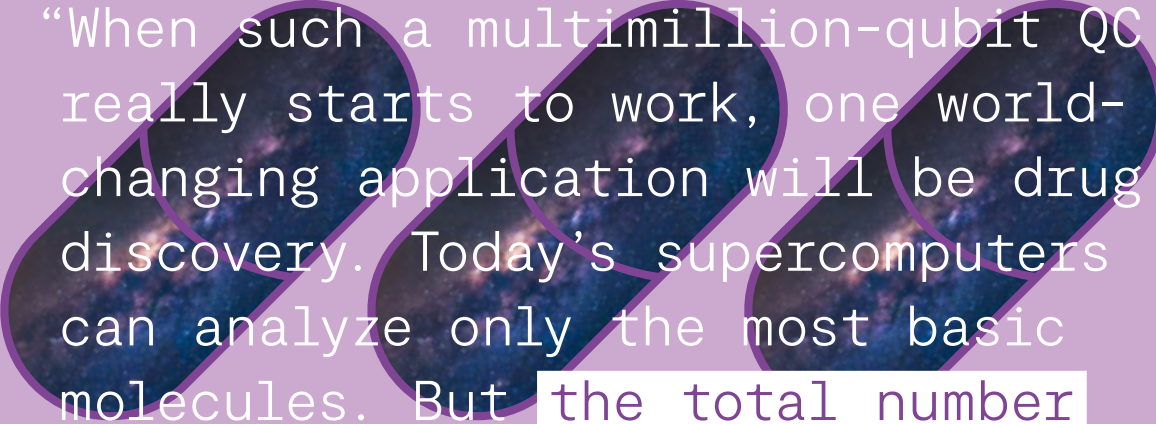
An IBM report concludes that "chemical discovery, product development, and process optimization are among the manufacturing areas" quantum computing is expected to disrupt.³⁰ The automotive, aerospace and electronics industries specifically would benefit from the development of "materials with more advantageous strength-to-weight ratios" (imagine if we could innovate something like spider silk, for instance) and enhanced, environmentally friendly catalytic processes.

Logistics and Supply Chain

Say goodbye to traveling salesman problems. Scheduling and routing shipments has always been a huge challenge for transportation companies, but the speed and power of QC will drive major new efficiencies into what was once a costly, complex operational challenge.²⁹ QC will also help manufacturers manage resource allocation and network design; it will also enable precise estimates of energy use in production facilities.

Digital transformation (DX) is massively changing not only how and how fast businesses can do things — it's fundamentally rewriting the book on what can be done. Now, add QC to the mix and buckle up. Quantum transformation (QX) is almost here.

Many organizations are pursuing an aggressive quantum development agenda, among them familiar names like Microsoft, Google, Intel, HP, Alibaba and IBM. There's also a host of brilliant new players whose names you don't know yet, but will soon.²⁶



“When such a multimillion-qubit QC really starts to work, one world-changing application will be drug discovery. Today’s supercomputers can analyze only the most basic molecules. But the total number of molecules that could make a drug is exponentially greater than all the atoms in the observable universe. Tackling a problem of this scale requires quantum computers, which will operate using the same quantum properties as the molecules they’re trying to simulate. QC can simultaneously simulate new compounds as new drugs, and model complex chemical reactions to it, to determine their efficacy.”

—Lee and Qiufan, AI 2041



Stop the Presses!

2021

2022

Just as this book was being finalized, IBM announced it was launching a 127-qubit quantum chip. Perhaps even more compelling was the news that they expect to introduce a 433-qubit chip in 2022 and another with 1126 qubits in 2023. The company said the processor would be available to select IBM Quantum Network customers starting in December 2021.

2023

01110010 01100001 01101110
01110011 01101111 01101101
01110111 01100001 01110010
01100101

Ransomware

*Somewhere in Europe, 120,000 BCE
Neanderthal sister to
brother: If you don't give
me your apple, I'll tell Mom
what you did.*

And so it began.



01110010 01100001 01101110 01110011 01101111 01101101 01110111 01100001 01110010 01100101

From Caesar to Cyberspace

00100000 01101111 01110010 00100000 01110011 01100011 01110101 01101100
00111000 01110011 01110000 00101100

As noted in our April 2021 Ransomware field guide the first recorded kidnapping case involved Julius Caesar.³¹ But the act of extorting – rooted in fundamental dynamics like greed and bullying – is so innately human it’s likely similar behaviors have been around as long as sapiens.

Or longer.

Macque monkeys will rob tourists and barter for the return of stolen items,³² so our fictional Neanderthal extortionist probably isn’t a stretch at all.

But what about the future?



Ransomware is an epidemic

One of the most prominent forms of cybercrime, it has been called the “go-to” tactic for hackers. Cybersecurity Ventures predicted ransomware’s toll to top \$20 billion in 2021.³³

Longer-term predictions are hard to pin down, but by 2030 its global cost could be in the trillions.

Ransomware is a form of cyber attack in which the target’s files are encrypted. Access is only restored when the victim pays the ransom.

We use the term extortionware here to refer to “cyber blackmail” or “double-extortion ransomware,” an insidious variation in which attackers threaten to release stolen data if their demands (usually, but not necessarily financial) aren’t met.

Garden-variety ransomware and extortionware aren’t mutually exclusive, of course: hackers can both ransom and extort with the same set of stolen assets (and frequently do).



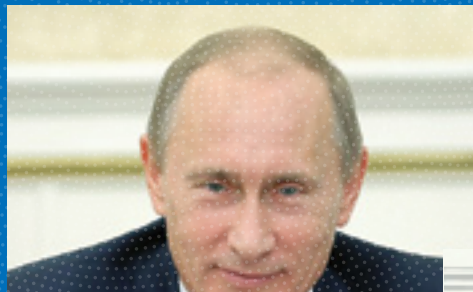
Extortion attacks can be devastating.

For instance:

- The release of customer data can expose a company to regulatory compliance charges and trigger massive brand damage.
- Businesses reliant on proprietary R&D (like tech or pharma enterprises) might be ruined if their trade secrets are revealed.
- Public figures like politicians, celebrities or corporate leaders could have careers destroyed by the publication of information revealing their involvement in illicit or illegal behavior.

Deepfake Ransomware

Deepfakes (deep learning + fake) use advanced technology to replace one person's likeness with that of another. Rudimentary forms of this practice have been possible for years thanks to digital image manipulation packages like Photoshop, but rapidly evolving AI/ML platforms now enable production of audio and video clips in which the deception is nearly undetectable.

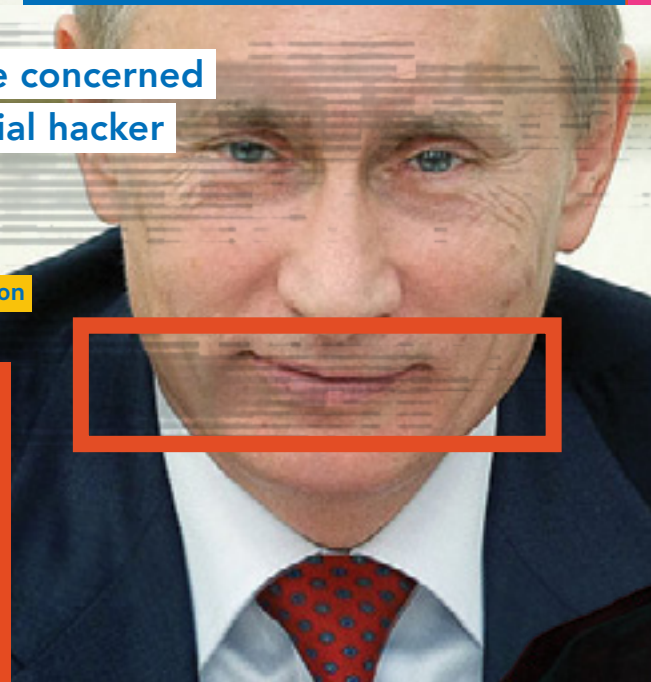


Cybersecurity experts are concerned about a variety of potential hacker deepfake applications.

For instance:

Political character assassination or manipulation

One obvious tactic, given recent concerns surrounding interference in US elections, involves the fabrication and release (or threatened release) of audio or video designed to damage a political aspirant. Such content might depict the politician engaging in objectionable acts or saying things antithetical to the electorate. These attacks might issue from any quarter – opposition parties, hacktivists, nation-states and even financially motivated criminals could benefit by threatening or damaging an office holder or candidate.



Blackmail, Stock + Brand Manipulation



Liked by user and others
username Hello! #social

A deepfaked business, analyst, media or regulatory persona (imagine DeepCramer, if you will) can be used to make public comments about companies in order to artificially damage (or boost) market or brand value. Similar goals can be pursued via deepfake bot swarms, where artificial identities are created and deployed across social platforms to manipulate public perception of brand popularity.

Similar to basic ransomware attacks noted above, deepfake technology will almost certainly be used (if it hasn't been already) to manufacture bogus audio or video of celebrities and public figures engaging in compromising activity. Since the damage to the target's career and reputation could be massive (fatal, even) the victims will have every incentive to quash the deepfake.

Theft

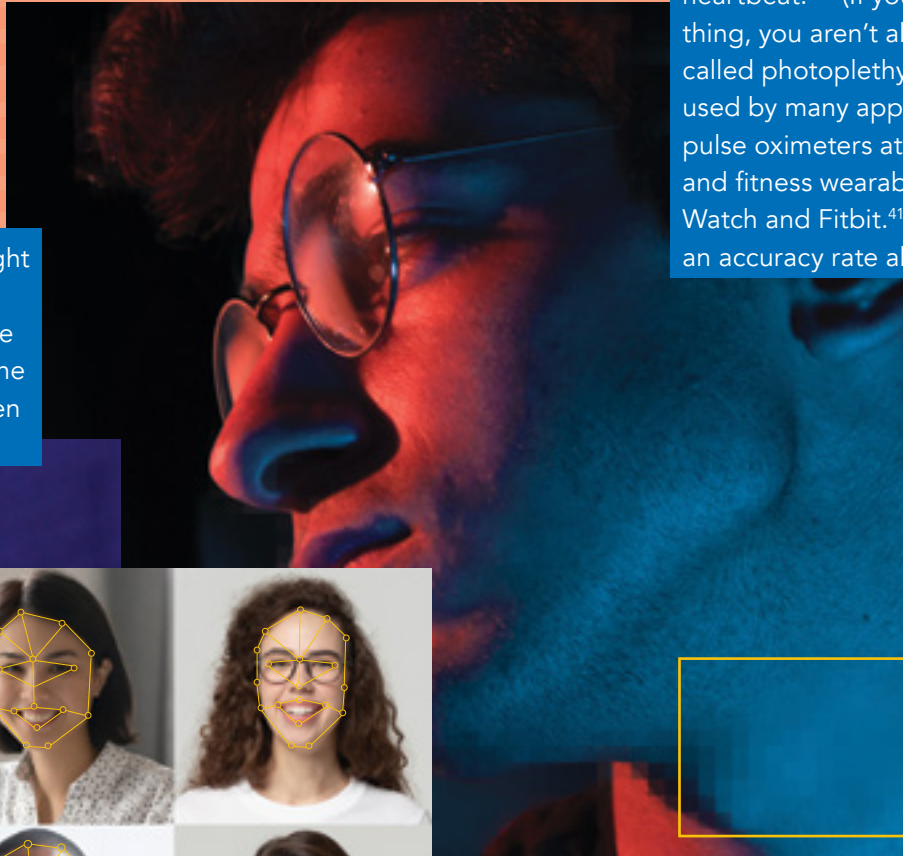
Attackers can use voice cloning or AI-powered face-swaps to impersonate an influential person (a corporate leader, for example). The faked persona can be used to initiate fraudulent financial transactions or gain access to sensitive information. This first happened (as best we can tell) in 2019, when a UK energy executive who thought he was talking to the CEO was duped into transferring \$243,000 to a "Hungarian supplier."³⁴

Then it happened again nine months later – to the tune of \$35 million.³⁵

Anti-Deepfakes

Tremendous effort is being devoted to the task of detecting and countering deepfakes...

A new **Microsoft** tool tries to spot signs (which might not be visible to the naked eye) "that an image has been artificially generated."³⁷ Tell-tales include "subtle fading or greyscale pixels at the boundary of where the computer-created version of the target's face has been merged with that of the original subject's body."



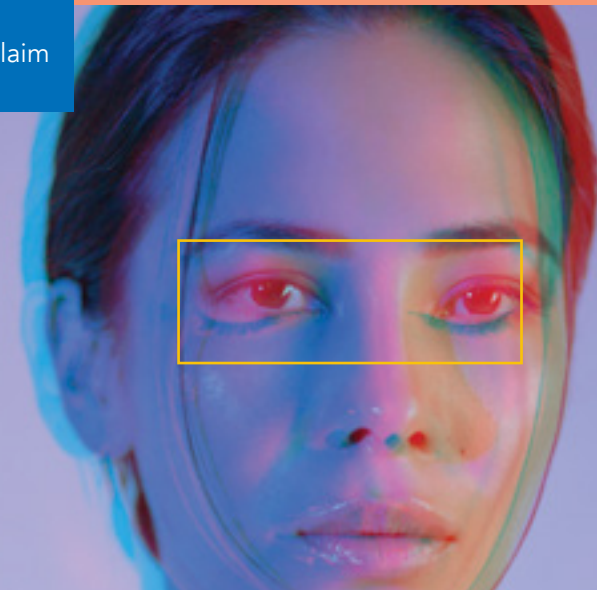
Facebook is also working to develop a new technique to reverse-engineer deepfakes and track their sources. Led by Michigan State University PhD student Vishal Asnani, this new technology seeks to identify the architectural traits of previously unknown deepfake models. "These traits, known as hyperparameters...leave a unique fingerprint on the finished image that can then be used to identify its source."

A team from **Intel** and Binghamton University examine "subtle differences in skin color caused by the human heartbeat."⁴⁰ (If you didn't know this was a thing, you aren't alone.) The technology, called photoplethysmography (PPG), is used by many applications, including pulse oximeters at your physician's office and fitness wearables like the Apple Watch and Fitbit.⁴¹ The researchers claim an accuracy rate above 90%.

94%



effectiveness of detecting deepfakes was achieved by University at Buffalo researchers by analyzing reflective patterns on the corneas.³⁴



Lionbridge AI catalogs a range of research, including tactics focused on analyzing facial and head movements as the subject speaks; eye aspect ratios (blinking patterns that factor in gender, age, activity and time); learning-based features employing convolutional neural networks; optical flow (looking for "discrepancies in motion across frames, such as unusual movements of facial parts"); and detecting imperfections inherent to the device manufacturing process.⁴²

Given the stakes, we can expect deepfake generation and detection innovation to escalate in coming years.

But...Will It Matter?

The most corrosive challenge posed by deepfakes, though, doesn't lend itself to a technical solution.

Recent decades saw ever-widening fissures in American society, with science/technology and the very nature of social reality serving as the battleground. In a "post-truth" world, where technical, rational and scientific evidence are routinely rejected according to ideological preconceptions, is there any reason to expect the solutions discussed here to affect audiences emotionally invested in a particular view?

A landmark 2019 study from the Pew Research Center found that "half of US adults say made-up news and information is a very big problem in the country today, and about two-thirds say it causes a great deal of confusion about the basic facts of current issues and events."⁴³

The problem, though, is the vast disagreement over what's factual and what's fictional. Huge swaths of the population simply don't trust science.

For instance: In the Pew report, more than a third of respondents said they think scientists disagree on climate change. They don't – nearly 95% say it's real and 87% attribute the disruption to human activity (only 50% of the public agrees).⁴⁴ Two-thirds thought scientists don't have a clear understanding of the health effects of genetically modified organisms. But 88% of scientists say GMOs are safe (only 37% of the public agrees); 68% of scientists say it's safe to eat foods grown with pesticides, but only 28% of the public agrees. (Both the GMO and pesticide dynamics are fueled, to some degree, by marketing campaigns touting "organic" agriculture.)

Public misunderstanding and "debates" also touch on any number of other issues, including vaccines, fluoridated water, evolution, whether the Earth revolves around the sun or vice versa (not making this up – 25% of Americans believe the latter) and pretty much anything with political implications. So what happens when a deepfake attacks a popular figure? Does the technical proof matter?

Knowledge Shortage?

Is this challenge related to education? Or do the causes run deeper? Dr. Adrian Bardon, a professor at Wake Forest University, says people are often driven by "motivated reasoning," a trait with deep history in homo sapiens.⁴⁵

Our ancestors evolved in small groups, where cooperation and persuasion had at least as much to do with reproductive success as holding accurate factual beliefs about the world. Assimilation into one's tribe required assimilation into the group's ideological belief system. An instinctive bias in favor of one's "in-group" and its worldview is deeply ingrained in human psychology.

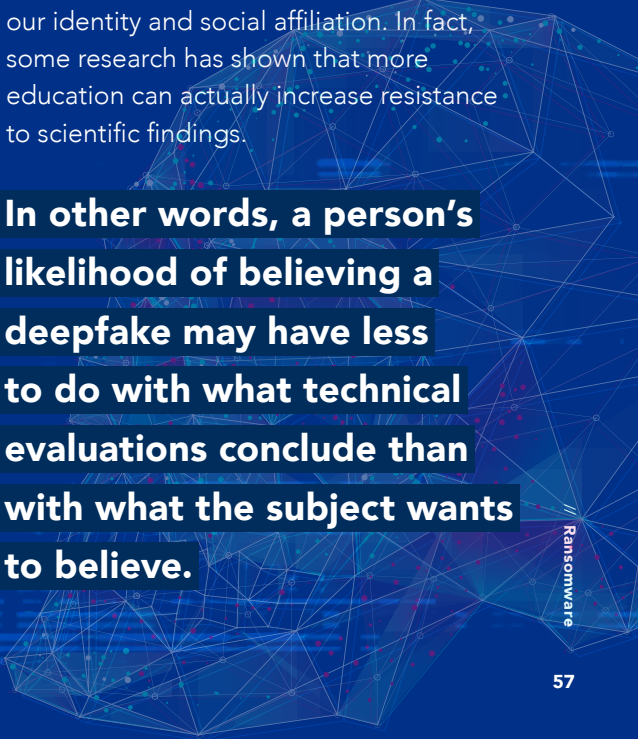
In our current context, acknowledging facts/truth about a hot-button issue has less to

do with lack of information or scientific consensus and more to do with political persuasion, which is a key element in our identity and social affiliation. In fact, some research has shown that more education can actually increase resistance to scientific findings.

In other words, a person's likelihood of believing a deepfake may have less to do with what technical evaluations conclude than with what the subject wants to believe.



A Visual Future of Cybersecurity Optiv



Ransomware

04

The future is already here — it's just
not very evenly distributed.
—William Gibson

The Ubiquitous Attack Surface

```
01010100 01101000 01100101 00100000 01010101 01100010 01101001 01110001  
01110101 01101001 01110100 01101111 01110101 01110011 00100000 01000001  
01110100 01110100 01100001 01100011 01101011 00100000 01010011 01110101  
01110010 01100110 01100001 01100011 01100101
```

```
01010100 01101000 01100101  
00100000 01010101 01100010  
01101001 01110001 01110101  
01101001 01110100 01101111  
01110101 01110011 00100000  
01000001 01110100 01110100  
01100001 01100011 01101011  
00100000 01010011 01110101  
01110010 01100110 01100001  
01100011 01100101
```



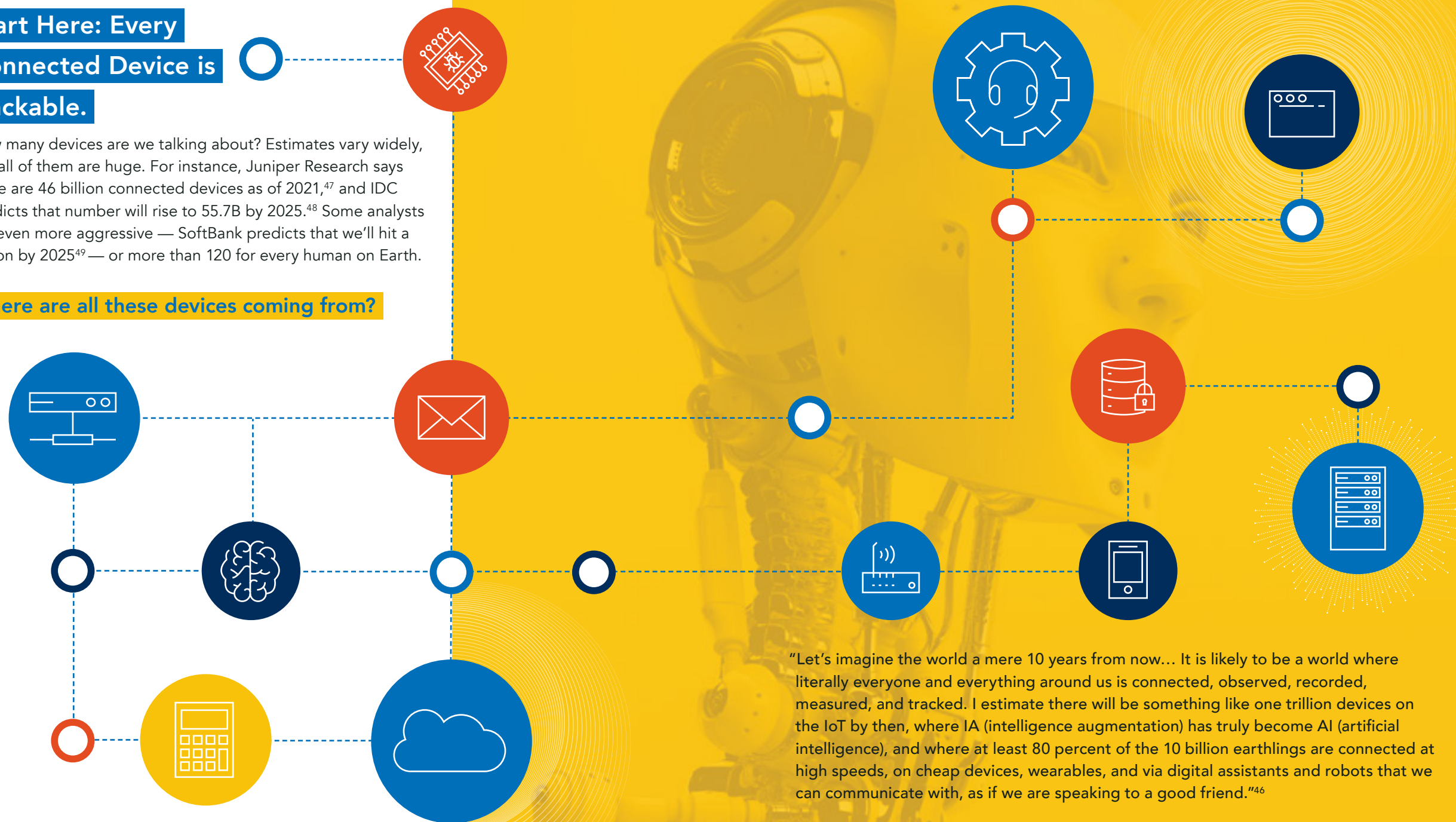

Once upon a time IT secured a server and some PCs in the home office and called it a day. Network expansion and the increasing need for remote access changed all that, though — work from home (WFH), field access by sales groups, bring-your-own-device (BYOD) policies, the need to connect third-party vendors and partners, the exploding demands of ecommerce, the growth of IoT and a lot more... Today's furiously evolving digital panorama means yesterday's defense strategies are deader than the phonebook.

So, what happened?

Start Here: Every Connected Device is Hackable.

How many devices are we talking about? Estimates vary widely, but all of them are huge. For instance, Juniper Research says there are 46 billion connected devices as of 2021,⁴⁷ and IDC predicts that number will rise to 55.7B by 2025.⁴⁸ Some analysts are even more aggressive — SoftBank predicts that we'll hit a trillion by 2025⁴⁹ — or more than 120 for every human on Earth.

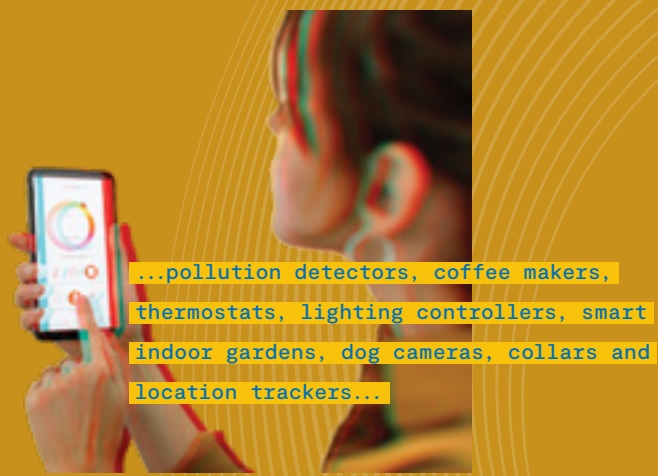
Where are all these devices coming from?



"Let's imagine the world a mere 10 years from now... It is likely to be a world where literally everyone and everything around us is connected, observed, recorded, measured, and tracked. I estimate there will be something like one trillion devices on the IoT by then, where IA (intelligence augmentation) has truly become AI (artificial intelligence), and where at least 80 percent of the 10 billion earthlings are connected at high speeds, on cheap devices, wearables, and via digital assistants and robots that we can communicate with, as if we are speaking to a good friend."⁴⁶

—Gern Leonhard
Chief Executive Officer, The Futures Agency

IoT is huge business, with consumer retail applications providing the most visible examples. The number of digital voice assistants in use worldwide will eclipse 6.4 billion units by 2022 and jump as high as 8 billion by 2023.⁵⁰



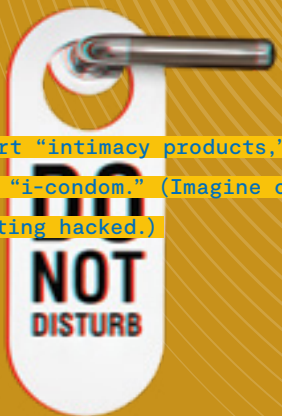
...pollution detectors, coffee makers, thermostats, lighting controllers, smart indoor gardens, dog cameras, collars and location trackers...



We now have smart everything, from watches, fitness wearables and refrigerators to doorbells and home alarm systems...



...internet-connected teddy bears and flip-flops, salt shakers and deodorant, dental floss, a smart belt and last, but certainly not least...



Assorted smart "intimacy products," including an "i-condom." (Imagine one of those getting hacked.)

Consumer gadgetry is just the beginning. Industrial systems feature devices allowing companies to monitor and regulate oil wells remotely, while Windows computers control nuclear plants and iPads tweak the pressure and temperature of offshore drilling rigs. Classic analog systems in manufacturing are being digitized and interconnected at warp speed. We bank and trade securities on our phones. Our health records are digital.

Before we move on, let's quickly call out an important force multiplier:

As IoT proliferates, ransomware (previous chapter) becomes more deadly.

It's one thing to lose your data but another if your electrical plant blows up or your autonomous car gets hijacked.

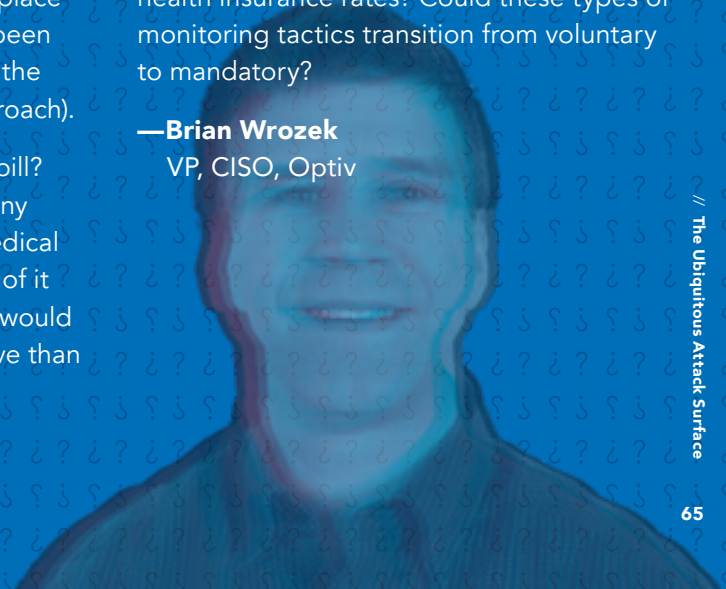
Let's Play What-If With the CISO

Maybe we eventually get to the point where we simply throw out and replace technology/gadgets rather than trying to patch them. Think of it as disposable technology. The security control is that it might be easier and cheaper to just replace it. We're already seeing some signs of this. It's quicker and simpler to replace containers with a new image that's been updated with the latest security (vs. the traditional scan-evaluate-patch approach).

What if you don't pay your medical bill? Could the OEM or insurance company remotely disable your implanted medical device until you pay your bill? Think of it as a form of legal ransomware. This would certainly be cheaper and less invasive than having it surgically removed.

Today, you can plug a monitoring device into your car that tracks your driving habits, with the potential reward of lower car insurance rates. Tomorrow, will I be able to upload exercise statistics from my watch or swallow a pill to share diet and nutrition information for the potential reward of lower health insurance rates? Could these types of monitoring tactics transition from voluntary to mandatory?

—Brian Wrozek
VP, CISO, Optiv



The Incredible Expanding Attack Surface

...a hyperconnected world could support up to 1 million devices per square kilometer with next generation cell phone systems (5G), compared with the 60,000 devices currently possible with current cell networks, with even faster networks on the horizon.⁵¹



These systems all talk to each other using software and the internet, expanding the attack surface in ways previously unimaginable. Add to the mix all the ways end users access such services, and it's evident that once-basic concepts like "network" and "endpoint" have gotten murky.



COVID, of course, accelerated attack surface diffusion. Organizations already kicking around cloud migration strategies before the pandemic found themselves needing to shift quickly. Remote work transformed overnight: what was a coveted perk for execs became a daily reality for millions of workers who, out of necessity, used mobile devices to access cloud resources.



In other words, our thinking about network perimeters, internal networks, endpoints, data centers and cloud services (and the way we secure them) is evolving – and it needs to evolve faster. A lot faster.

1M devices per square km

Expanding Inward

This paradigm shift isn't just about the sheer number of devices, either — the scope is expanding. Consider the Internet of Medical Things (IoMT) and the increasingly intrusive character of innovation. For instance, some digital technologies are “on-board” — as in, they reside *inside* the body.

Coming soon to a hospital near you...

There's every reason to expect this trend to accelerate, especially since these technologies save lives and improve patient quality of life.

01000001 01101100 01101100 00100000 01101100 01101001 01100110 01100101 00100000
01110111 01100001 01110011 00100000 01110111 01101111 01101110 01100100 01110010
01101111 01110101 01110011 00101100 00100000 01110001 01110101 01101001 01100011
01101011 00101100 00100000 01100101 01101100 01100101 01100011 01110100 01110010
01101001 01100011 01100001 01101100

It gets better.

Salim Ismail of the ExO Foundation explains:

“...the potential for dynamic disruption expands exponentially, accelerated by the shift from the read phase of digitization to the write phase.

In this next phase, we are talking about the capability of **writing code to our bodies, brains and genomes.**”

2022



“On-board”
medtech is
a reality.

2024



From a biotech
standpoint, we are
probably within
**two years of more
widespread deployment.**

2028



From a neuro-science
standpoint, we are
perhaps **five or six
years away.**

1.25M

pacemakers are implanted each year worldwide (as of 2019) and the billion-dollar market for infusion pumps is growing at nearly 6% annually.⁵²



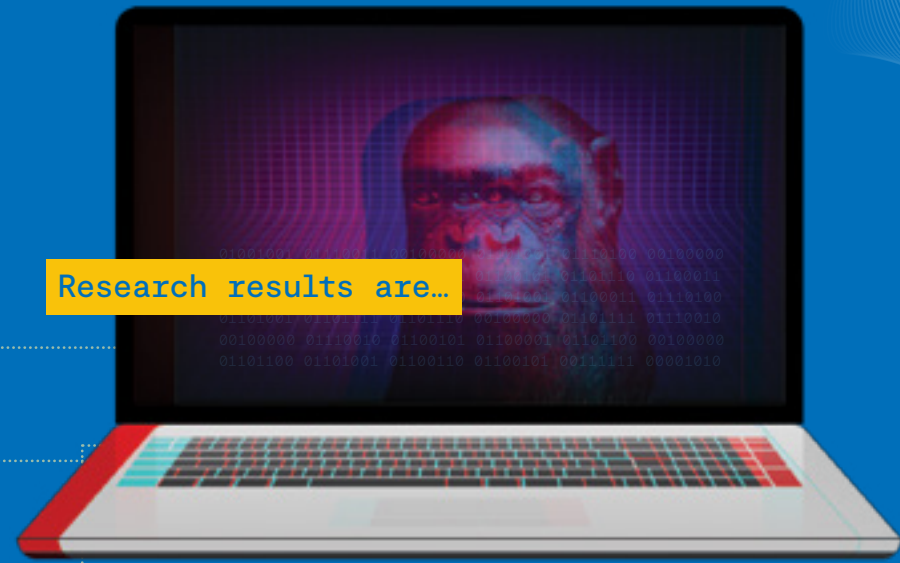
// The Ubiquitous Attack Surface

We're Just Getting Started

In fact, organizations like Neuralink and Synchron are already pushing the envelope into decidedly “science fiction” territory. (Thanks to CEO Elon Musk’s public profile, Neuralink is the best-known player in the sector, but Synchron actually beat Neuralink to FDA approval for brain-computer interface human trials.)⁵³

Neuralink’s brain-machine interface (BMI) tech, which implants a small device in the skull (they embedded an AI chip in a pig in 2020), is designed to treat serious brain diseases in the near term.⁵⁴

The company hopes to eventually cure millions worldwide suffering from Alzheimer’s and movement disorders (Parkinson’s, Huntington’s Disease, Dystonia, Lewy Body Dementia, Tourette Syndrome, the dozens of Ataxia variants, etc.).



Research results are...

well, science fiction.

In April of 2021 Neuralink released video footage showing a monkey playing a video game with its mind. And a 2020 Synchron experiment “successfully allowed two paralyzed people to control computers with just their thoughts.”

This is incredibly promising for clinical applications. But you may have noticed that word “game.” In addition to the BMI’s medical benefits, the potential recreational applications are as lucrative as they are numerous. How soon can expect to see BMI-powered first-person shooters transforming the gaming industry?

And remember – every brain with an implant is a node on the attack surface.

Flying

Microchips?

Northwestern University engineers recently announced development of unpowered microdrones they say are the smallest-ever human-made flying structures.

Inspired by the maple tree's whirly-gigging propeller seeds, these devices would be dropped from an aircraft and stay aloft for "extended periods," thanks to interactions with "ambient wind."⁵⁵

The wind would scatter the tiny microchips, which could sense their surrounding environments and collect information. The scientists say they could potentially be used to monitor for contamination, surveil populations or even track diseases.

According to the Federal Aviation Administration, there were 871,006 drones (aka unmanned aircraft systems [UASs] or unmanned aerial vehicles [UAVs]) registered in US as of June 2021, with slightly more than 40% being commercial.⁵⁶ (Hobby drones weighing less than 250 grams don't have to be registered.)



Not surprisingly, the number of drones is expected to grow, but how much? Estimates vary, but Thomas Frey, founder of the DaVinci Institute, told the World of Drones Congress there will be a billion unmanned vehicles by 2030 – although not all of them will be flying.⁵⁷

" They can also roll on the ground," he noted. "They can stick to the side of a building, float in the river, dive under water ... they can climb a tree and attach themselves like a parasite to the side of a plane. A driverless car is a drone."

Much of this explosive growth simply boils down to fun, but the technology demonstrates tremendous benefit and utility, driving commercial innovation and adoption.⁵⁸

Current uses include:

Retail In the very near future we expect autonomous vehicles to be delivering everything from pizza to your latest Amazon order.

Emergency Response and Rescue Sometimes emergency situations represent significant danger to rescuers. In cases like drownings, avalanches and forest fires, drones can save lives and prevent property damage without putting more people than necessary at risk.

Wildlife Conservation It's nearly impossible for humans to track animal populations, but UAVs make it easy to keep tabs on "orangutans in Borneo ... bison on the Great Plains"⁵⁸ and more. They're also a potent weapon in the war against poachers in Asia and Africa. (We're big fans of that last bit, especially.)

Ecology ~300 million acres have been reforested by UAVs since the early 1990s — a task it would have taken human workers three centuries to accomplish.

Historical Conservation UAVs can "map out 3D renderings of historical sites like Chernobyl, the ancient Greek sites of Ephesus, Turkey and Jewish cemeteries all over Europe."⁵⁸ Thanks to drones, preservation and archaeological experts can gather useful information about culture and architecture and virtually recreate lost sites.

Medical UASs can cheaply and effectively deliver medicines to remote patients and are already being used to deliver organs to transplant patients.

Agriculture Global population continues to grow and climate change represents an increasing threat to food production. But UAVs can help with early disease detection, crop yields, planting, soil maintenance, pesticide application and irrigation.⁵⁹

Photography Hey, I wonder what that looks like from 2,000 feet?⁶⁰

And this is all happening **right now**.

Just imagine what **the future** is going to be like.⁶¹

Science! Drones already make possible the exploration of hostile environments on Earth — like deep oceans. In the future we'll see deployment of more unmanned vehicles, like NASA's Intrepid copter on Mars and the even larger Dragonfly, which will begin exploring Titan (Saturn's largest moon) in 2036.⁶² Expect to see UAVs being developed by private enterprises as well, with an eye toward asteroid mining.

Flying Taxis! Volocopter is set to launch a drone taxi service in Singapore by 2024.⁶³

Robot Bees! Bee populations, which are essential for pollination, are endangered, threatening agriculture around the world. Enter miniature pollinator drones.⁶⁴

Flying Watchdogs! Know what your home alarm system is missing? Remote autonomous drones.⁶⁵

3D-Printed Skyscrapers! Can you imagine a construction drone printing building components as it flies? No need to — it's already in development.

Professional Drone Wrestling! Okay, we made this one up. But why not? The Drone Racing League is already a thing and there's no reason emerging technologies can't be adapted for all kinds of must-see sports and entertainment competitions, right? (This seems like something our flourishing sports betting industry would be all-in on.)

News, Sports and Drone Weather at 11! Weather forecasting is mostly a function of information, and in recent years we've gotten far better at gathering and processing meteorological data. Satellites, radar and weather balloons tell us a lot, but often there's crucial missing info inside a storm.⁶⁶ UAVs will fly us right into the thick of things without risking anyone's well-being, harvesting data that may prove critical to developing life-saving forecasts.

Killbots! As of 2019 there were believed to be at least 21,000 UAVs in service to more than 100 militaries globally.⁶⁷ A majority are non-combat models, but armed UAVs have been

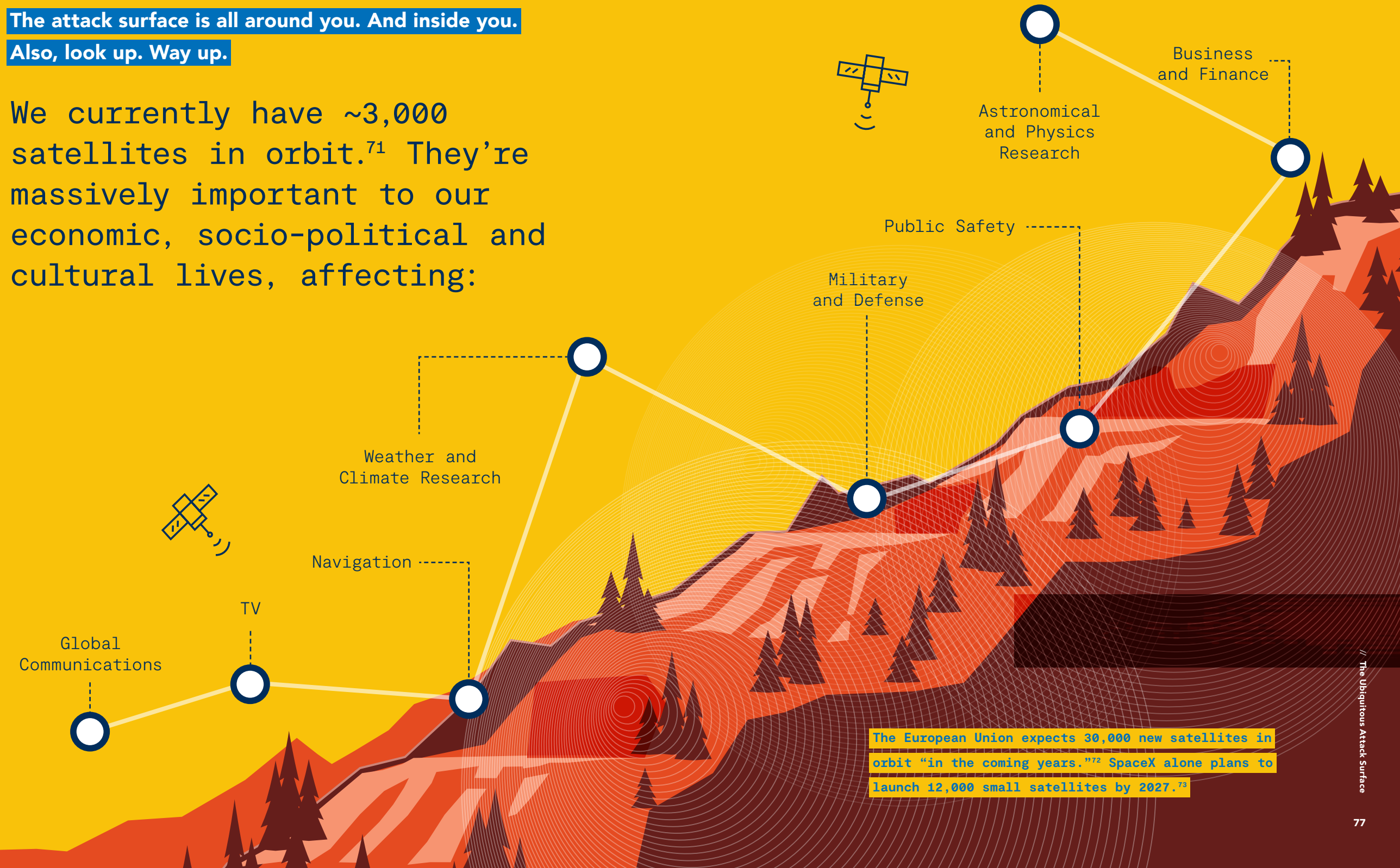
deployed around the world since the early 21st century (and are thought to be in the arsenals of more than three dozen nations, including traditional powers like the US, China and Russia as well as less obvious players like Turkmenistan, Kazakhstan and Greece).⁶⁸ Experts say the rapid growth of UCAV development and use is inevitable.

Autonomous Killbots! AI-powered drones can navigate and operate without human intervention. In a military (or police, or terrorist) context, this means the UAV can be authorized to make attack/kill decisions. (We're not 100% sure, but this may already have happened)⁶⁹

Autonomous Killbot Dog-fights! DARPA is working on a "counter-drone" that shoots "stringy streamers" at enemy drones to knock them out of the sky.⁷⁰

The attack surface is all around you. And inside you.
Also, look up. Way up.

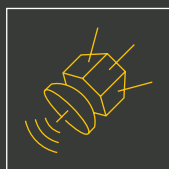
We currently have ~3,000 satellites in orbit.⁷¹ They're massively important to our economic, socio-political and cultural lives, affecting:



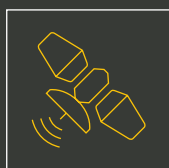
The European Union expects 30,000 new satellites in orbit "in the coming years."⁷² SpaceX alone plans to launch 12,000 small satellites by 2027.⁷³

Space Economy

The (projected \$2 trillion) “space economy”⁷⁴ is like any other digital technology system in that all assets are vulnerable to cyberattacks.⁷⁵ Worse, threats to satellites also place related terrestrial critical infrastructure at risk, potentially endangering global economic development and international security. Referencing an Aerospace Corporation report,⁷⁶ Wilson Center analysts say:



Spacecraft could be vulnerable to command intrusions (giving bad instructions to destroy or manipulate basic controls), payload control and denial of service (sending too much traffic to overload systems). Malware could be used to infect systems on the ground (like satellite control centers) and for users, and links between the two and spacecraft could be spoofed (disguising communication from an untrusted source as a trusted one) or suffer from replay (interrupting or delaying communication by malicious actors).



A significant weakness of satellite systems is their reliance on long-range telemetry for space-to-ground communications, which often employ easily accessible open-network security protocols.



Satellite ground stations are particularly vulnerable – if a malicious actor is able to interrupt the satellite signal they may be able to gain access to any downstream systems connected to the satellite. In this way, an attacker could potentially trespass through an organization’s network starting from the infiltrated satellite ground station.



Military-grade communications must comply with Commercial Solutions for Classified Program (CSfC) requirements, but commercial satellites are also at risk. Some smaller companies may not adequately prioritize cyber defense.

“Cybersecurity thought leaders can’t just focus on the technical dimension of technology. If we don’t take an active role in the political and social conversations we risk letting people who don’t understand the tech or the issues, people with no regard for the good of society, set the agenda.”

—Brian Wrozek
VP, CISO, Optiv

Challenges and Solutions of a Dispersed Attack Surface



Challenge: Code

The way software developers build and ship code frustrates security pros. Many developers rely on third-party libraries to build applications, plugging prefabricated chunks of code together like Lego blocks.

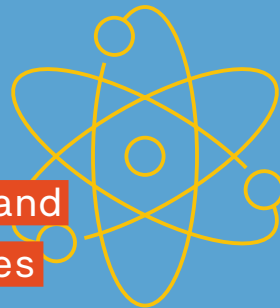
The resulting Frankencode might harbor any number of vulnerabilities, complicating the job of the cyber team. Worse, the push toward DevSecOps plus business-side pressure to ship code faster fans the flames, making it difficult to insinuate even basic levels of security into the dev process.

From the lay perspective, it's all about the sexy tech – pizza delivery drones, satellites, implanted medical devices, etc. But the cybersecurity battle is mostly fought under the hood.

We asked our experts to overview some of the main challenges in dealing with the ubiquitous attack service in the coming years ... and also where the solutions lie.

Challenge: Serverless and Microservices

Many applications come pre-bundled with all the code files they may (or may not) need to work with the various infrastructures floating around in the world, and this diffusion of code sources creates problems for security. Outsourcing server security to cloud providers has an upside, but CISOs and their teams need to keep a sharp eye on all app components, paying close attention to how they interact with each other. (And don't even get us started on third parties.)



Challenge: APIs and RPAs



Speaking of the ways systems interact, application programming interfaces (APIs) and robotic process automation (RPA) are really what make distributed computing tick. APIs lay the groundwork for integration and from there the sky's the limit for what we can make applications do. And where there aren't APIs, RPAs can perform tasks autonomously.

The possibilities are endless, but aren't without risks. Who has access to your APIs? How can we be sure your provider's API is secure and protecting your data? What can the RPA access? Managing these risks begins with understanding them.

Which brings us to the “security wild card:” users. As they leave the network’s proverbial castle walls, it’s more important than ever for employees to get the message that their behavior matters. Building a culture of security means users know the risks and take responsibility for their use of the system⁷⁷. Cybersecurity cultures don’t evolve where there’s friction, so organizations should provide secure, seamless access to their resources. (Done right, we can prove that security makes the job easier.)

Solutions

AppSec (Code, Microservices, APIs): “Shift left, defend right” means introducing security earlier in the development process. This lets developers address security concerns proactively rather than reactively (like after an eventual security review cycle). It’s about understanding what’s in your application. Easier said than done, we know, but a software bill of materials (SBOM) must be a key component of secure code-building.

Identity: Thanks to attack surface dispersion, it doesn’t make sense anymore to manage access to resources from the resource’s perspective. Now it’s better to shift the lens to identity and access management, which focuses on the entities (the users, devices and automated processes) looking to gain access. By creating a unique digital identity and set of permissions for each entity, organizations can maintain ultimate control of the system and provide a seamless user experience at the same time. Identity, for instance, can reduce the number of times users have to enter their passwords, thus reducing friction (while improving security). Emerging models like Zero Trust provide a framework to employ identity along with other core security concepts.

Evolving Cybercrime Models

01000101 01110110 01101111 01101100
01110110 01101001 01101110 01100111
00100000 01000011 01111001 01100010
01100101 01110010 01100011 01110010
01101001 01101101 01100101 00100000
01001101 01101111 01100100 01100101
01101100 01110011

"It was the ultimate irony. Hackers get into hacking because they don't want desk jobs — but all hacking is a desk job."
—Brad Meltzer



01000101 01110110 01101111 01101100 01101110 01101001 01101110 01100000 01000011
01110110 01100010 01100101 01100010 01100011 01100010 01100011 01101101 01100101 00100000
01001101 01101111 01100100 01100101 01101100 01110011

Ransomware's technical innovation is unnerving, but the business practices enterprises and collaborating in ways that improve efficiencies, cybercriminals are evolving scale and customization, are arguably the bigger story. Savvy hacker organizations are increasingly able to operate as securely and profitably as many real companies.

The May 2021 hack of Colonial Pipeline (and dozens of other organizations) by a Russian syndicate known as DarkSide cast hard light on perhaps the most insidious cyber attack strategy to date: Ransomware as-a-Service (RaaS). And thanks to RaaS authors leasing their user-friendly products on the dark web, it no longer takes a skilled hacker to perform such an attack. That's right — the market is now wide open to garden-variety criminals as well, dramatically increasing the world's viable threat actor population and helping supercharge the trillion-dollar cost predictions in the previous chapter.

DIY

RaaS operations don't typically conduct cyberattacks. Instead, they provide hackers with the technology and services needed to do it themselves.



An RaaS affiliate might receive:

Code

How-to guides and technical support

Negotiation handling and “customer support”(to help victims submit the ransom)

Payment processing services

Clearinghouse for stolen information

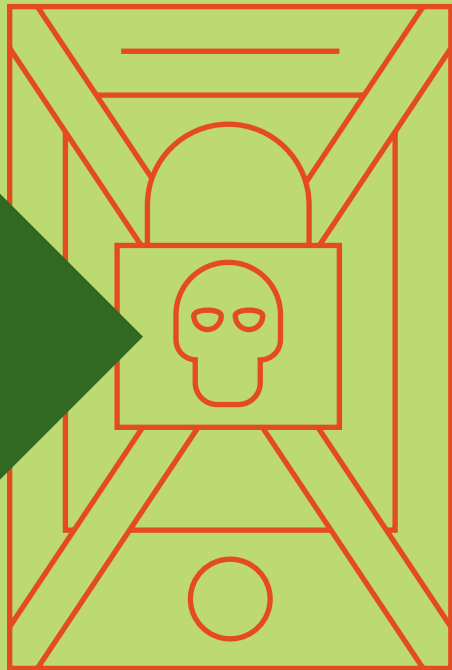
Common RaaS revenue models⁷⁸ will look familiar to anyone who does legitimate business online:

Flat-fee monthly subscription

Affiliate programs (like the monthly fee model, but with a percent of the profits [usually 20-30%] going to the RaaS provider)

One-time license fee/no profit sharing

Pure profit sharing (with sliding scale structures based on size of ransom)



RaaS providers can have employees (engineers, leaders, developers, etc.), costs, profits and most other things we associate with actual companies. (It isn't clear if they also offer health insurance, PTO, 401K sharing or health club memberships.)

Industry analysts, whose predictions are routinely validated by real-world attacks (like Colonial Pipeline), expect RaaS business models to evolve toward “big game hunting” – fewer, better vetted hacks seeking higher payouts from victims with deeper pockets.

CaaS

Ransomware as-a-Service is part of a booming corner of the cybercrime world: Cybercrime as-a-Service (CaaS), aka Malware as-a-Service (MaaS).

CaaS platforms are typically simple to use and emphasize the customer experience, driven by "user-friendly administration consoles and dashboards to control the earnings."⁷⁹

In addition to RaaS, the CaaS umbrella covers things like:

- 1 **Phishing as-a-Service.**⁸⁰ PhaaS is helping fuel the number one cause of breaches worldwide. Google identified well over 2.1 million phishing sites as of January 2021 – a 27% year-over-year increase.⁸¹
- 2 **Deepfakes as-a-Service.** Real-time DaaS hasn't been demonstrated yet, although more primitive versions are in the wild⁸² currently and it's hard to imagine hackers not taking advantage of a technology that could allow them to defeat authentication procedures protecting, for instance, cryptocurrency accounts.
- 3 Other examples include⁸³ subscriptions to modular malware services, the purchase of cheap Neutrino exploit kits and the ability to rent Mirai devices (to set up botnet hacks), DDoS booters and advanced malware packages.⁸⁴

How and how effectively hackers can use artificial intelligence in the future is still an open question (see chapter 1 discussion). But if attackers can demonstrate its effectiveness (i.e. profitability), AI as-a-Service offerings for cyber criminals seem likely.

Hacker Collaboration

Cyber attackers have apparently decided they're all on the same team. Analysts note that cooperation (formal and informal) between gangs on tool sharing, exploits, vulnerabilities, exploitation infrastructure and any other information that might be helpful. But that's barely the tip of the iceberg.

If the idea that global cybercrime syndicates might be taking cues from the successes of Silicon Valley and the VC world is ... bracing, at least it suggests an important future direction for cybersecurity pros.

"Cybercriminals have discussed, in open forums, proposals to create a venture capital organization or stock market of sorts, where interested parties can finance the development of malware, tools, and frameworks without ever writing a line of code."⁸⁵



All Hands on Deck

Everyone writing their own scripts on how to deal with the same threat is analogous to every building hiring and managing its own unique fire department. Where's the sense in that? More importantly, where's the true sense of collaboration, cooperation and public-private partnership to fight this growing issue?

Attackers have created their own criminal ecosystem in which they do a spectacular job sharing information, resources and expertise. If our adversaries have a strategy of collaboration and shared interest, then shouldn't we respond with a similar strategy? Shouldn't our response be *e pluribus unum* all over again — out of many, one? We need to forge a highly functional cyber-defense ecosystem that encompasses government and all public and private sector organizations to match the criminal ecosystem we're facing every day.

“Beyond the simple call to do the right thing, we need to embrace the fact that helping other industry participants helps everyone in the long run as we reduce the efficacy of the threat and ultimately reduce their level of capitalization. Collaboration isn't just the right thing to do, it's also the smart thing to do. We must inspire companies to come together, work together and problem-solve together.”⁸⁶

—Kevin Lynch
CEO, Optiv

In “Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers,” **Sherri Ramsay, former director of the NSA’s Threat Operations Center**, is even more blunt:

“If you’re not collaborating with colleagues and competitors on cyber threat intelligence, beware: the bad guys are way ahead of you.”⁸⁷

She references several existing laws and frameworks, including the Information Sharing and Analysis Center (ISAC), Comprehensive National Cybersecurity Initiative (CNCI) and The Cybersecurity Act of 2015, but notes that, “we have talked about information sharing, but we have not yet done nearly enough to dramatically move the needle in our favor.”

Why do they collaborate? Why do they share? The answer is simple. It saves them time and it saves them money. According to Etay Moor, Senior Strategist at IBM, “Information sharing is a given on the dark side of the net.” That’s a big reason the average cost of conducting an attack is decreasing and attacks are spreading across networks at a faster pace, year after year.



THE OLD MODEL NO BE SURE TO DRINK LONGER WORKS YOUR OVALTINE



Ramsay offers “pragmatic, hard-headed, enlightened” collaboration and crowdsourcing as a strategy for countering cyber attackers. She concludes by making clear that the “old model for cybersecurity no longer works. It’s broken, and it can’t be fixed.”

Keeping an incident quiet or sharing only among a few friends potentially exposes others to the same attack, which is a fundamental breach of fiduciary responsibility, whether you’re a CEO, board member, CISO or government official. A true exchange – a connective defense – will

give our organizations the best opportunity not only to defend our digital infrastructure against attacks, but it also will enable others to understand the threat landscape and help all of us.

Ramsay is echoed in the May 2021 White House Executive Order on Improving the Nation’s Cybersecurity (EO),⁸⁸ which specifically calls out the current failure to share critical information. At present many cyber attacks go unreported (often due to fears that transparency might damage the brand). When hack details are kept secret it benefits attackers – widespread sharing of attack

information would simplify the challenge of defending against cyber criminals.

The EO mandates sharing of intel by enterprises doing business with the Federal Government. It’s not clear that a broader requirement compelling transparency in all cases will be forthcoming, but it’s something to watch for.

Sherri Ramsay

Former Director, NSA’s
Threat Operations Center

How High are the Stakes?

Gartner® predicts⁸⁹ that, “By 2024, a cyberattack will so damage critical infrastructure that a member of the G20 will reciprocate with a declared physical attack.” This feels both “FUDdy”⁹⁰ and hyperreal, which is unique for our private entities.

For the first time since Rosie the Riveter, private industry is playing a real part in the defense of our country. As Gartner notes in a 2021 press release⁹¹:

“In the near-term, enterprises will continue to bear the primary responsibility to defend against cyberattacks. However, enterprises have never been charged with serving as the first line of defense against warfare, so increasingly severe attacks will prompt military involvement, eventually deterring non-state actors from targeting critical infrastructure.”

Everyone knows our utilities (oil, electric, water, telco) and supply chain (food, goods, logistics) have vulnerabilities, but communicating risk in this area is always a challenge — especially when board and CFO risk models break. In these cases the odds are low, but the consequences are potentially lethal (see also, Oldsmar water hack)⁹² and measured in the billions (see also, Colonial Pipeline).⁹³

The risk gets magnified when you consider the rapid pace of connectivity. Seven years ago, most of our critical infrastructure sites were offline. Today, most of these sites can stream Netflix from control centers. Threat actors are active here and looking for holes during this migration.

“Key takeaway: Rosie the Riveter needs a CISSP.”

—Sean Tufts

Demand & Delivery Director, Cyber Digital Transformation, Optiv



The future
always comes
too fast
and in the
wrong order.

—Alvin Toffler

01101010 11110110 10010110 11001110 10101110
00110110 11100010 01110110 11110110 11100010

Conclusion

01100011 01101111 01101110
01100011 01101100 01110101
01110011 01101001 01101111
01101110

Once Upon a Time the Future Was in, Well, the Future.



OLD FUTURE

This isn't snark. Before the second half of the 20th century our technological fantasies — flying cars, space travel, robots, etc. — occurred decades out.



NEW FUTURE

No longer. Today, staggering innovation may be only months away. If we don't make it a point to pay close attention, we may discover that it already happened. A basic nuance of our modern world is that the word "future" doesn't mean quite what it used to.

Which means we have to be more attuned than ever to the horizon. When ideas go from conception to diffusion seemingly overnight, it means threats can be on you before you know it. And to Toffler's point, any cybersecurity pro can explain how threats usually arrive before solutions.

It's Critical to C-FAR

It takes more than tech to win a cyberwar. It takes the proper mindset.
A future-built mindset.

With such a mentality in place and in play, we can deal not just with a future or even a set of futures... we're better prepared for any future.

Optiv fosters a future-built mindset with our C-FAR ["see far"] framework, which emerges from and stands atop four fundamental pillars.

Clarity

An objective and complete view of one's environment, allowing for informed and decisive action

Foresight

Cultivated and honed by strategically looking down the board and around corners

Agility

A highly adaptive and dynamic stance to match a tumultuous world, reflected in systems, culture and security posture

Resilience

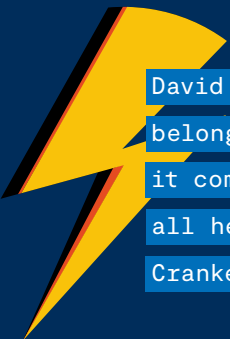
Forging the ability to competently weather and withstand threats and attacks

C-FAR not only means you have your eyes on the road ahead, but also on the big picture. "The new now" is a thicket of threats, but you don't have to go into the dark forest alone.

We're your trusted cyber advisor and solutions partner, providing direction through this chaotic terrain and helping you forge a future-ready mindset and organization.

[Learn more about C-FAR](#) →

We encourage our clients, colleagues and communities to think forward, think fast and think broadly. Study tomorrow as a matter of habit. Study yesterday to make sure nothing important got past you. And, as Brian Wrozek says above, get involved in shaping public and policy conversations so that our shared future benefits everyone.



David Bowie said the future belongs to those who can hear it coming. If we listen, we can all hear it. In surround sound. Cranked to 11.

We manage
cyber risk so you
can **secure your**
full potential



The background of the image features a series of concentric circles in a lighter shade of blue, centered on a solid blue background. The circles are thin and closely spaced, creating a subtle ripple effect.

Secure greatness™

References

1. "Thought Leadership and Science Fiction," Optiv, Nov 19, 2020 <https://www.optiv.com/insights/discover/blog/thought-leadership-and-science-fiction>

2. Kai-Fu Lee & Chen Qiufan, AI 2041 <https://www.amazon.com/AI-2041-Ten-Visions-Future/dp/059323829X>

3. Dave DeWalt, OptivCon, Nov. 2020 <https://gateway.on24.com/wcc/experience/optiv/1237620/2759031/optivcon-virtual-november>

4. The State of AI in 2020, McKinsey, Nov. 17, 2020 <https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/global-survey-the-state-of-ai-in-2020>

5. "Artificial Intelligence Market, Markets and Markets <https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-market-74851580.html>

6. Global Trends 2040: A More Contested World, National Intelligence Council https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf

7. Artificial Intelligence as Security Solution and Weaponization by Hackers, Dec. 9, 2019 <https://cisomag.eccouncil.org/hackers-using-ai/>

8. Ibid

9. 2021 Cyber Threat Trends Outlook https://boozallen.com/content/dam/boozallen_site/ccg/pdf/publications/cyber-threat-trends-outlook-2021.pdf

10. Tay [https://en.wikipedia.org/wiki/Tay_\(bot\)](https://en.wikipedia.org/wiki/Tay_(bot))

11. Bias in Artificial Intelligence <https://www.harvardmagazine.com/2021/08/meredith-broussard-ai-bias-documentary>

12. Cybercrime, Meet AI, TechNative, Nov. 7, 2019 <https://technative.io/cybercrime-meet-ai/>

13. AI Wrote Better Phishing Emails Than Humans in a Recent Test, Wired, Aug. 27, 2021 <https://www.wired.com/story/ai-phishing-emails/>

14. Google's Quantum Computer Is About 158 Million Times Faster Than the World's Fastest Supercomputer, Medium, Feb. 28, 2021 <https://medium.com/predict/googles-quantum-computer-is-about-158-million-times-faster-than-the-world-s-fastest-supercomputer-36df5674717f>

15. China Claims Fastest Quantum Computer in the World, LiveScience, Dec. 7, 2020 <https://www.livescience.com/china-quantum-supremacy.html>

16. Post-Quantum Cryptography, NIST <https://csrc.nist.gov/projects/post-quantum-cryptography>

17. The Clock Is Ticking for Encryption, ComputerWorld <https://www.computerworld.com/article/2550008/the-clock-is-ticking-for-encryption.html>

18. How a Quantum Computer Could Break 2048-Bit RSA Encryption in 8 Hours, MIT Technology Review <https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/>

19. Quantum Computing and Cybersecurity, Belfer Center for Science and International Affairs, July, 2021 <https://www.belfercenter.org/publication/quantum-computing-and-cybersecurity>

20. 1978 Cryptosystem Resists Quantum Attack, MIT Technology Review <https://www.technologyreview.com/2010/08/18/26136/1978-cryptosystem-resists-quantum-attack/>

21. Google's 'Time Crystals' Could Be the Greatest Scientific Achievement of Our Lifetimes, The Next Web <https://thenextweb.com/news/google-may-have-achieved-breakthrough-time-crystals/amp>

22. Observation of Time-Crystalline Eigenstate Order on a Quantum Processor, <https://arxiv.org/pdf/2107.13571.pdf>

23. Otherworldly 'Time Crystal' Made Inside Google Quantum Computer Could Change Physics Forever, LiveScience, Sep. 14, 2021 <https://www.livescience.com/google-invents-time-crystal>

24. AMD Files Teleportation Patent to Supercharge Quantum Computing, PC Gamer, Sep. 3, 2021 <https://www.pcgamer.com/amd-teleportation-quantum-computing-multi-simd-patent/>

25. There's Been Another Huge Quantum Computing Breakthrough, TechRadar, Sep. 9, 2021 <https://www.techradar.com/news/theres-been-another-major-quantum-computing-breakthrough>

26. What is Quantum Computing? Top 18 Quantum Computing Companies, Predictive Analytics Today <https://www.predictiveanalyticstoday.com/what-is-quantum-computing/>

27. How Quantum Computing Could Be One of the Most Innovative Climate Change Solutions? World Economic Forum, Dec. 17, 2019 <https://www.weforum.org/agenda/2019/12/quantum-computing-applications-climate-change/>

28. Chemistry is Quantum Computing's Killer App, Chemical & Engineering News, Oct. 30, 2017 <https://cen.acs.org/articles/95/i43/Chemistry-quantum-computings-killer-app.html>

29. Quantum Computing Applications for Supply Chain, Clarkston Consulting <https://clarkstonconsulting.com/insights/quantum-computing-applications-sc/>

30. Exploring Quantum Computing Use Cases for Manufacturing, IBM <https://www.ibm.com/downloads/cas/LJBOKBLW>

31. Ransomware: Yesterday, Today, Tomorrow <https://www.optiv.com/insights/discover/downloads/cybersecurity-field-guide-5-ransomware-yesterday-today-tomorrow>

32. Monkey Mafia Steal Your Stuff, Then Sell It Back for a Cracker, New Scientist, May 25, 2017 <https://www.newscientist.com/article/2132748-monkey-mafia-steal-your-stuff-then-sell-it-back-for-a-cracker/>

33. Global Ransomware Damage Costs Predicted to Reach \$20 Billion (USD) by 2021, Cybersecurity Ventures, Oct. 21, 2019 <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/>

34. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case, Wall Street Journal, Aug. 30, 2019 <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>

35. Deepfaked Voice Enabled \$35 Million Bank Heist in 2020, Unite.ai, Oct. 15, 2021 <https://www.unite.ai/deepfaked-voice-enabled-35-million-bank-heist-in-2020/>

36. Deep Learning for Deepfakes Creation and Detection: A Survey, Apr. 26, 2021 <https://arxiv.org/pdf/1909.11573.pdf>

37. Deepfake Detection Tool Unveiled by Microsoft, BBC News, Sep. 1, 2020 <https://www.bbc.com/news/technology-53984114>

38. Facebook Develops New Method to Reverse-engineer Deepfakes and Track Their Source, The Verge, June 16, 2021 <https://www.theverge.com/2021/6/16/22534690/facebook-deepfake-detection-reverse-engineer-ai-model-hyperparameters>

39. Scientists Developed a Clever Way to Detect Deepfakes by Analyzing Light Reflections in the Eyes, The Next Web, <https://thenextweb.com/news/ai-detects-deepfakes-analyzing-light-reflections-in-the-cornea-eyes-gans-thispersondoesnotexist>

40. Best Way To Detect 'Deepfake' Videos? Check for the Pulse, NewsWise, Oct. 27, 2020 <https://www.newswise.com/articles/best-way-to-detect-deepfake-videos-check-for-the-pulse>

41. A Review on Wearable Photoplethysmography Sensors and Their Potential Future Applications in Health Care, National Institutes of Health, Aug. 6, 2018 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6426305/>

42. Lionbridge <https://lionbridge.ai/articles/three-types-of-deepfake-detection/>

43. Americans' Struggles With Truth, Accuracy and Accountability, Pew Research Center, July 22, 2019 <https://www.pewresearch.org/politics/2019/07/22/americans-struggles-with-truth-accuracy-and-accountability/>

44. Americans Believe in Science, Just Not Its Findings, The Atlantic, Jan. 29, 2015 <https://www.theatlantic.com/health/archive/2015/01/americans-believe-in-science-just-not-its-findings/384937/>

45. Humans Are Hardwired To Dismiss Facts That Don't Fit Their Worldview, The Conversation <https://theconversation.com/humans-are-hardwired-to-dismiss-facts-that-dont-fit-their-worldview-127168>

46. The Def initive Cybersecurity Guide for Directors and Officers, Security Roundtable <https://www.securityroundtable.org/navigating-the-digital-age-3rd-edition/>

47. How Many IoT Devices Are There in 2021? [All You Need To Know], TechJury, Nov. 1, 2021 <https://techjury.net/blog/how-many-iot-devices-are-there/>

48. IoT Growth Demands Rethink of Long-Term Storage Strategies, says IDC, IDC, July 28, 2020 <https://www.idc.com/getdoc.jsp?containerId=prAP46737220>

49. Softbank Believes 1 Trillion Connected Devices Will Create \$11 Trillion in Value by 2025, VentureBeat, Oct. 16, 2018 <https://venturebeat.com/2018/10/16/softbank-believes-1-trillion-connected-devices-will-create-11-trillion-in-value-by-2025/>

50. Share of Questions Answered Correctly by Selected Digital Assistants as of 2019, by Category, Statista <https://www.statista.com/statistics/1040539/digital-assistant-performance-comparison/>

51. Global Trends 2040: A More Contested World, National Intelligence Council https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf

52. Intravenous Infusion Pumps Market Size, Share & Trends Analysis Report by Product (Volumetric, Insulin, Syringe, Enteral, Ambulatory, Implantable Pumps), by Disease Indication, by Region, and Segment Forecasts, 2021 - 2028, Grand View Research, Aug. 2021 <https://www.grandviewresearch.com/industry-analysis/intravenous-infusion-pump-market#>

53. Synchron Beats Musk's Neuralink To FDA-Approved Brain-Computer Interface Human Trials, IFL Science, July 30, 2021 <https://www.iflscience.com/brain/synchron-beats-musks-neuralink-to-fdaapproved-braincomputer-interface-human-trials/>

54. Elon Musk's Neuralink Could Transition From Implanting Chips in Monkeys to Humans Within the Year, Business Insider, Apr. 12, 2021 <https://www.businessinsider.com/elon-musk-predicts-neuralink-chip-human-brain-trials-possible-2021-2021-2>

55. Flying Microchips The Size Of A Sand Grain Could Be Used For Population Surveillance, NPR, Sep. 23, 2021 <https://www.npr.org/2021/09/23/1040035430/flying-microchip-sand-grain-northwestern-winged>

56. UAS by the Numbers, Federal Aviation Administration <https://www.faa.gov/uas/resources/by-the-numbers/>

57. One Billion Drones by 2030?, Flying, Aug. 31, 2017 <https://www.flyingmag.com/one-billion-drones-by-2030/>

58. Drones, BuiltIn <https://builtin.com/drones>

59. 10 Ways Drones Will Be Used in The Future, Drone Tech Planet <https://www.dronetechplanet.com/10-ways-drones-will-be-used-in-the-future/>

60. Best Drone Photos Ever: Stunning Images Taken From the Sky, Pocket-Lint.com, Oct. 27, 2021 <https://www.pocket-lint.com/drones/news/133911-best-drone-photos-ever-stunning-images-taken-from-up-high>

61. 7 Different Uses for the Future of Drones, DataFloq, Apr. 30, 2018 <https://datafloq.com/read/7-different-uses-for-the-future-of-drones/4936>

62. Mars Ingenuity Helicopter: Why Drones Are the Future of Space Exploration, Science Focus, Apr. 11, 2021 <https://www.sciencefocus.com/news/mars-ingenuity-helicopter-why-drones-are-the-future-of-space-exploration/>

63. Flying Taxis Will Launch in Singapore and Paris by 2024, Gent, Apr. 12, 2021 <https://generationasia/ideas/flying-taxis-singapore-paris>

64. Pollination Drones Seen as Assistants for Ailing Bees, Robotics Business Review, Mar. 27, 2018 <https://www.roboticsbusinessreview.com/agriculture/pollination-drones-assist-ailing-bees/>

65. Sunflower Labs <https://www.sunflower-labs.com/>

66. 10 Ways Drones Will Be Used in The Future, Drone Tech Planet <https://www.dronetechplanet.com/10-ways-drones-will-be-used-in-the-future/>

67. Nearly 100 Countries Have Military Drones, and It's Changing the Way the World Prepares for War, Business Insider, Sep. 27, 2019 <https://www.businessinsider.com/world-rethinks-war-as-nearly-100-countries-field-military-drones-2019-9>

68. Who Has What: Countries with Armed Drones, New America <https://www.newamerica.org/international-security/reports/world-drones/who-has-what-countries-with-armed-drones/>

69. AI Drone May Have 'Hunted Down' and Killed Soldiers in Libya With No Human Input, LiveScience, June 3, 2021 <https://www.livescience.com/ai-drone-attack-libya.htm>

70. DARPA's Interceptor Drone Shoots "Stringy Streamers" To Drop Enemy Drones, The Drive, June 8, 2021 <https://www.thedrive.com/the-war-zone/40982/darpas-interceptor-drone-shoots-stringy-streamers-to-drop-enemy-drones?fbclid=IwAR23AzJy18O61xFoVKln8x1tesDL4kFKcTWSNjHpFF2Dz8f1df17R9G1o>

71. Thousands More Satellites Will Soon Orbit Earth – We Need Better Rules to Prevent Space Crashes, The Conversation, Jan. 28, 2021 <https://theconversation.com/thousands-more-satellites-will-soon-orbit-earth-we-need-better-rules-to-prevent-space-crashes-154014>

72. Speech by Commissioner Thierry Breton at the 13th European Space Conference, European Commission, Jan. 12, 2021 https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/speech-commissioner-thierry-breton-13th-european-space-conference_en

73. The Number of Satellites Orbiting Earth Could Quintuple in the Next Decade, MIT Technology Review, June 26, 2019 <https://www.technologyreview.com/2019/06/26/755/satellite-constellations-orbiting-earth-quintuple/>

74. The Big 3 Stocks to Buy for the Emergence of the \$2 Trillion Space Economy, Investor Place, Jan. 19, 2021 <https://investorplace.com/hypergrowthinvesting/2021/01/space-stocks-to-buy-trillion-dollar-opportunity/>

75. Cybersecurity Threats in Space: A Roadmap for Future Policy, Wilson Center, Oct. 8, 2020 <https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy>

76. Defending Spacecraft in the Cyber Domain, Aerospace Corporation, Nov. 2019 https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf

77. National Cybersecurity Awareness Month and Cybersecurity Culture, Optiv, Oct. 15, 2019 <https://www.optiv.com/insights/discover/blog/national-cybersecurity-awareness-month-and-cybersecurity-culture>

78. CrowdStrike, Jan. 28, 2021 <https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/>

79. The Crimeware-as-A-service Model Is Sweeping Over the Cybercrime World. Here's Why. CyberNews, Oct. 16, 2020 <https://cybernews.com/security/crimeware-as-a-service-model-is-sweeping-over-the-cybercrime-world/>

80. This Is Not a Drill: Phishing as-a-Service, Optiv, Nov. 7, 2019 <https://www.optiv.com/explore-optiv-insights/blog/not-drill-phishing-service>

81. Must-Know Phishing Statistics: Updated 2021, Tessian, Sep. 16, 2021 <https://www.tessian.com/blog/phishing-statistics-2020/>

82. Deepfakes as a Service, Recorded Future, Feb. 22, 2021 <https://www.recordedfuture.com/podcast-episode-197/>

83. Giuliano Liguori, June 4, 2020 <https://twitter.com/ingliguori/status/1268431722905042948>

84. What Is Cybercrime as a Service? MakeUseOf, Apr. 25, 2021 <https://www.makeuseof.com/what-is-cybercrime-as-a-service/>

85. 2021 Cyber Threat Trends Outlook, Booz Allen Hamilton https://boozallen.com/content/dam/boozallen_site/ccg/pdf/publications/cyber-threat-trends-outlook-2021.pdf

86. Incenating A Collaborative Approach To Putting Out Cyber Fires, Forbes, Aug. 31, 2021 <https://www.forbes.com/sites/forbestechcouncil/2021/08/31/incenating-a-collaborative-approach-to-putting-out-cyber-fires/>

87. The Definitive Cybersecurity Guide for Directors and Officers, Security Roundtable <https://www.securityroundtable.org/navigating-the-digital-age-3rd-edition/>

88. Executive Order on Improving the Nation's Cybersecurity, May 12, 2021 <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

89. Gartner Press Release, "You'll Be Breaking Up with Bad Customers-and 9 Other Predictions for 2022 and Beyond," Oct. 19, 2021 <https://www.gartner.com/en/articles/you-ll-be-breaking-up-with-bad-customers-and-9-other-predictions-for-2022-and-beyond>

90. Fear, Uncertainty and Doubt, Wikipedia https://en.wikipedia.org/wiki/Fear_uncertainty_and_doubt

91. Gartner, "Gartner Unveils Top Predictions for IT Organizations and Users in 2022 and Beyond," Oct. 19, 2021, <https://www.gartner.com/en/newsroom/press-releases/2021-10-19-gartner-unveils-top-predictions-for-it-organizations-and-users-in-2022-and-beyond>

92. A Hacker Tried to Poison a Florida City's Water Supply, Officials Say, Wired, Feb. 8, 2021 <https://www.wired.com/story/oldsmar-florida-water-utility-hack/>

93. Colonial Pipeline Ransomware Attack, Wikipedia https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

Thank You

WRITING + EDITING

Sam Smith, PhD
Evans Mehew

TECHNICAL CONSULTING

Eric DiPietro
Zak Nelson

DESIGN

Rachel Briggs
Melina Chastain
Rafael Encarnacion
Joel Hawkins
Michael Hill
Kaitlan Kelly
Martha LeBlanc
Matthew Watkins

CONTRIBUTORS

Brian Wrozek
Sean Tufts
Randy Lariar
Luis Jiminez

PROJECT MANAGEMENT

Kelly Weinland
Sarah Hite
Deborah Baker
Charleigh Loder

CREATIVE DIRECTION

Jeanne Bacque
Joel Hawkins
Kaitlan Kelly
Ruben Mercado

EDITING SUPPORT

Michael Clark
Jennifer Peranteau
Clarke Reader
Steve Wilke

EXECUTIVE SUPPORT

Heather Rim



AN OPTIV
PUBLICATION

Cybersecurity Field Guide Series



Keep up to speed with the latest strategies and tactics for securing your environment.

[Check out the series](#) —>

Secure greatness™

Optiv Security is the cyber advisory and solutions leader, delivering strategic and technical expertise to more than 7,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential.

©2021 Optiv Security Inc. All Rights Reserved. Optiv is a registered trademark of Optiv Inc.

Optiv Global Headquarters
1144 15th Street, Suite 2900
Denver, CO 80202

800.574.0896 | optiv.com