Volume Forty, Number Two
DIGITAL EDITION

2600

The Hacker Quarterly

International Payphones

Uruguay. These are four (supposedly) working and clean phones as seen at the Buquebus terminal in Colonia. They're either very well maintained or completely forgotten.

Photo by Arturo "Buanzo" Busleiman

India. Seen at the Indira Gandhi International Airport in New Delhi, this phone gives you the opportunity to get a printed receipt for your call! Retro and modern simultaneously.

Photo by Jack Jordan

Kazakhstan. Spotted in a bank of three at an Almaty subway station. Two were out of service. It takes only cards, which are rather hard to find and not sold in the station. (That logo for Kazakhtelecom sure does look familiar.)

Photo by Babu Mengelepouti

Japan. While payphones are still somewhat common here, this bank of them found on one of the Shinkansen platforms at Kyoto Station really stands out. For one thing, the sunlight seems to be highlighting their bright green cases. A sight to behold.

Photo by maroth

Got foreign payphone photos for us? Email them to payphones@2600.com. Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (more photos on inside back cover)

Categories

omnishambles

Artificial Nonsense

These are fun times to be in the world of high tech. We've been around for some of the more dramatic landscape shifts starting with the breakup of the Bell System to the explosion of personal computers, development and commercialization of the Internet, as well as the fun and peril that social media has brought to us. (In all of these, incidentally, hackers were considered to be the biggest threat.)

Now it appears we're seeing the ground shake yet again with the exponential use and popularity of artificial intelligence and chatbots. And as with every technological development that has come along in the past half century, there are those who live in fear and dread of what's about to happen and those who look forward to the fun and chaos. Count us amongst the latter.

First, some words of advice. Please don't think of artificial intelligence as anything more than a potentially useful tool. It's not actually intelligent and is basically nothing more than formulaic responses to specific requests using a massive dataset of words, facts, and narratives. You can program this tool to say things that will make it appear human, but it is no more human than ELIZA was decades ago on mainframes. In fact, just as you could program a calculator to give wrong answers (something we'd really enjoy having around the office), so too could a chatbot exist that's designed to be completely unhelpful and even destructive. Such a thing could be achieved with either very good or very bad programming.

We've already seen a number of instances of the latter. A chatbot named Tessa was brought in by the National Eating Disorders Association (NEDA) to replace their hotline workers a mere four days after they had unionized. There's a lot we can say about NEDA's motivations here, but let's move forward a bit to see what wound up happening. A mere week after this decision was made, Tessa had to be taken offline after it was found to be suggesting unhealthy eating habits and actually supporting eating disorders to the very people who needed exactly the opposite advice. One user was quoted in *Motherboard* as saying "Every single thing Tessa suggested were things that led to the development of my eating disorder. This robot causes harm."

We even saw a rather humorous example of this directed at *2600* where it was claimed by Google Bard that a documentary film titled *2600: The Hacker Quarterly* had been made in 2012 to rave reviews ("A fascinating and thought-provoking look into the world of hackers" according to *The New York Times* and other similar praise from different publications). The chatbot also provided a very specific list of theaters it had played in from Hollywood to Hong Kong, and even informed us that the DVD/Blu-ray release was on October 16, 2012. The more questions we asked, the more detail we received, such as: "The film has been praised by critics for its balanced and informative approach to the subject of hacking. It has also been praised for its interviews with some of the most influential figures in the hacker community."

Of course, not one word of this was true. No such film has ever been made. But it sounded quite believable. Bard even went so far as to credit specific real people with this release. One would not be wrong to define this as pathological lying - if this was actually done by a human. But, of course, it wasn't. This kind of behavior can only be attributed to the design and training of the chatbot in question.

We found this to be funny because we knew not to take it seriously. This is a technology in its infancy and it's going to screw things up. A lot. And it's up to us to push it to the limits and figure out ways to break it. That's what hackers do, after all.

We are most certainly not at the dawn of a robot uprising or the singularity, despite the panic you may be hearing from people, many of whom really should know better. How much power we give to AI bots is entirely up to us. Every instance of something going wrong with artificial intelligence can be traced directly back to a human messing up and believing that automation was an acceptable substitute

for human interaction and decision making.

None of this is meant to imply that artificial intelligence can't pose a very real threat to our daily lives. But that will only come about if we or the people we entrust make very bad decisions. An autonomous car, for instance, may indeed have a better safety record than a vehicle driven by a human. But if we stop encouraging humans to learn how to drive, they will become wholly dependent on automation in order to go anywhere, which will become a huge problem if something goes wrong with that system, as it inevitably will.

A tool is only great if you truly know how to use it. If you can't operate without it, you literally have become an extension of the tool, rather than the other way around. And that means you might never know when it's giving you bad results and you certainly won't know why.

In May, approximately 4,000 jobs in the United States were lost to artificial intelligence. This represents around five percent of the total amount of jobs lost for that month. Earlier in the year, Goldman Sachs predicted that 300 million jobs worldwide would eventually be replaced by artificial intelligence. At press time, there was an ongoing strike involving the Writers Guild of America where one of the major issues was the increasing use of AI to produce written content.

This is a true concern if replacement by AI is the end of the story. And all of this clearly shows one thing: humans are the problem. We don't mean that in the sense that they do inferior work and need to be replaced by something better. The problem lies in those humans who believe in AI so much that they're willing to have their fellow humans replaced by code and routines that clearly are not up to the task.

When a company replaces its work staff with artificial intelligence, they are basically saying that they no longer have to actually care. What other message can be inferred from those who no longer want to actually *talk* to their customers? It might be possible to fool many into thinking they're having a real conversation, but the reality is they're not and the many benefits of actual interaction will never be realized. Subtleties in the back and forth will be missed, suggested improvements and corrections by the customer will be ignored, and those priceless human connections that we can never predict simply won't be made. That is the world where artificial intelligence is seen as a replacement.

What can be said for us if we allow secret algorithms to determine who we are and what we like? This has already been happening everywhere from Facebook to Netflix and it's considered normal and even convenient. That's on us for accepting someone else's interpretation of our very beings and not demanding that these systems work the way we as individuals want them to. But now the very real possibility exists that such algorithms will be used by film and television studios to *create* new works based on what we have already accepted. They're counting on us to not know the difference because it sure would save them a ton of money if we didn't. That's why we have to work harder to act more human and embrace the different and unique material, not just more of the same with slight variations. There's a real parallel to what makes a healthy society here.

So, yes, there is a threat here and not an insignificant one. But it's a threat that we are making to ourselves if we act lazy and allow the technology to be abused. The world where artificial intelligence is viewed as an enhancement to the work that humans are doing is one where we all can benefit. Jobs that don't require any actual thought are certainly better off being done by non-sentient automation. But the benefits realized must be passed on to those who are displaced, either through new and better jobs or adequate compensation from the savings being achieved. Generative AI is actually predicted to be a huge generator of employment, so there is really no excuse for anyone to be hurt by these advancements. Other than greed.

We know this is going to be challenging. But we also know that humans have a uniqueness to them that, while able to be imitated, will never be completely replicated. It might be a bit difficult on the surface to tell the difference, but that won't be the case when we spend a little more time listening and analyzing.

In other words, we need to simply pay more attention to each other. Then we'll truly know who we're talking to.

Programming of the Past

by Albert Einstable

I belong to the generation of programmers who contributed to the development of information technology when it was still called "automatic processing of information" in the 1980s, when mainframe systems were programmed pending the first personal computers.

The operating systems were very generic and not very personalized and the customizations were made by us programmers with very long and boring lines of code initially in assembler, then FORTRAN, COBOL, PL/I, and RPG, in particular in this case on IBM systems (System/360, System/32, System/34, System/36, System/38, up to AS/400). We can say that we were the first to do something by generating those program lines that today we could call the first hackers.

To give an example, to generate program lines in assembler, each field (data or numbers) to be used in the program itself had to be declared in the opening in the registers, but above all "clean" as if they were boxes to be prepared for subsequent processing. But the declarations, the dimensions, and the cleanliness of the field had to take into account whether you worked or would have worked with integers, decimals, alphanumeric, text; but also the presumed lengths of both integers and decimals, obviously also including the fields that would have been generated as results from the elaborations.

You can imagine what it meant with complex programs when the fields to be declared had to take into account input fields, constants, processing fields, transformation fields, and output fields for hundreds of fields and constants of a single program.

And this is where the true story of the first hackers begins, which I would say was born out of necessity and therefore with a small ethical semblance.

To generate these programs, it sometimes took days or weeks of work by a programmer, also because in the tests the famous "overflow" errors often occurred, i.e., incorrect declarations of the fields, which depended on the variables and constants entered.

Once the program was completed and tested, the source lines were "compiled" and transformed into an object program (not editable). While the source remained the property of the programmer or his company, the compiled object program was transferred and installed to the customer. The source program was practically never left to the customer, except in exceptional cases, but in any case the complexity made any attempt to manipulate third parties useless (there were at least thousands of lines of code, sometimes tens of thousands).

It sometimes happened that the customer did not pay, or delayed the payment, or no longer paid the balance or maintenance after purchasing the program or going into litigation for some other cause. How would you protect yourself from these risks? Simply by inserting lines of hidden code in routines that could generate an overflow error in the presence of a certain event, so that the programmer needed to intervene with the source to return a new compiled object program.

Malware routines were called in the presence of, for example, a calculation like this:

```
IF (uyear-xy)> 2 then execute
➥'routine-x'
```

where uyear was the year of the system (not editable because taken from the operating system), while xy contained a variable calculated by the program itself in subroutines which could be an event counter or a variable that could be set from a hidden field or from a calculation made by the serial number of the software which resulted in the number of years in which the guarantee of operation was desired. In this case, after two years the program called the routine "x" which suddenly overflowed the program, while showing a message of "call for assistance." The most common overflows were given by declaring an integer field and then processing it in decimal, so that the decimal part was seen as "overflow error."

I am aware that it was a trivial and perhaps not very intelligent solution, but always consider that we were precursors and only custodians of computer programming in a world where programmers hardly existed yet.

Even today, these subtle systems are widespread among teenagers, video game programmers, or even, it turns out, on large systems or companies that use programmers that develop software independently, in the event that the source code part is not intended for sale to the customer.

Science Fair and Congressional Farce

by Anthony Parr

My first foray into coding was on an 8086 before we installed the daughter board, and it was in BASIC. DOS was my playground and BASIC was my jungle gym. As a kid, I wrote loops and basic "If-Then" statements for fun. My dad had a programming book from his college and I just copied code out to puzzle the manner in which it worked. So in sixth grade, back in 1986, I used this book and this 8086 to create a super simple choose-your-own-adventure game. Personal computers were rare, so after creating my game I entered it into the school science fair.

It was an underwhelming success. The excitement that I held was dashed by the utter incomprehensibility of what I had created for the science fair judges. My story was something they could relate to and I tended to think in black and white at the time, so I slapped together a nice little tale of science versus technology. Everyone enjoyed the narrative and seemed to enjoy making the choices that took them down various paths. However, when I showed them my code, they were flummoxed. It was depressing. These were very intelligent and capable adults, who, unfortunately, had yet to be exposed to software code, just software. They swept my efforts in coding aside, gave me a ribbon, and moved on.

The reason I share this tale of "innocence lost" is that we now see congressmen in the news talking about applications and software such as TikTok, and how that software has access to the Internet. Now, we are not delving into transcoding, editing, or overlays. We are talking about whether or not TikTok, the app, *has access to your local Internet*. What in the world is our government looking for? Why are they not informed? The professional, intelligent, and capable adults in our government are behaving in the same manner as my science fair teachers in the sixth grade when faced with something they just don't grok.

This article's position is not to posit that all government leaders take coding classes or edit raster images in Gimp on their personally compiled flavor of Linux, but rather that they become informed by surrounding themselves with *objective* experts. However, since we are all working hard to pay the bills, it will probably be up to ChatGPT to solve these problems in the future. Hopefully, we can all put Dr. Sbaitso behind us.

A CHAIN ADDITION GENERATOR IN AWK

by Thumos

Justin Parrott's articles on keyspace iterators using AWK (issue 38:3) and port scanners in bash (issue 39:4) inspired me to try to stretch my scripting muscles. Several months back, I'd fallen down the Wikipedia rabbit-hole and stumbled upon the VIC cipher[1]. I was intrigued by the cipher's use of chain addition as a sort of lagged Fibonacci generator[2] and decided to see if I could write a chain addition generator in AWK.

The result is slow (almost seven minutes to create a 100M file) and not remotely close to cryptographically secure, but I considered it more an exercise in AWK than in cryptography. An earlier version had the user input both the number of rounds and the key as command line options. However, on a Linux system, this would leave the key in the user's shell history file, so I rewrote the script to ask for user input after it starts.

[1] en.wikipedia.org/wiki/VIC_cipher

[2] en.wikipedia.org/wiki/Lagged_Fibonacci_generator

The script:

```
#!/bin/awk -f
#chain-add : A chain addition generator
#Thanks to Justin Parrott for the inspiration
BEGIN {
printf "Enter number of rounds: ";
getline rounds < "/dev/stdin";
printf "Enter key: ";
getline key < "/dev/stdin";
split(key, num, "");
len = length(num);
for (i=1;i<=rounds;i++){
num[len+i] =
((num[i]+num[i+1])%10);
printf num[len+i]};
print}
```

Quantum Computer Algorithms

Part II: Amplitude Amplification

by Dave D'Rave

In the academic literature of quantum algorithms, you will often encounter a class of functions called "the oracle." These are gate sets which (potentially) have a large number of inputs and only one output, such that the output is interpreted as either being "Yes" or "No."

In the formalism, there are n active inputs, plus an input which has been set to |0>, and the oracle operates by performing a conditional-not on the |0> input, which may cause it to become non-zero.

As a practical matter, what usually happens is that the controlled-not is subject to some superposition of states, and that the output is something like k (|0> + 0.00001 |1>).

This can become large and complicated. For example, let's say that you have a (classical) oracle which is mining Bitcoin. You give it the current working block and a 32-bit nonce. The output will be 1 if the output hash is below the threshold, and a 0 otherwise. Strictly speaking, if you have a quantum oracle doing the same thing, it will produce the same results, which is kind of pointless.

More interesting is if I build a quantum Bitcoin oracle, and then send it the current working block and a superposition of, say, 64 nonce values. The output will then either be |0>, if none of the proposed nonce values is good, or (0.992 |0> + 0.125 |1>), if one of the nonce values is good and the others are bad. (For now, we are not interested in cases where more than one nonce is good.)

This looks like a step forward, in that we now have a factor of 64 reduction in work. The problem is that it is not easy to tell the difference between a |0> output state and a non-zero output state.

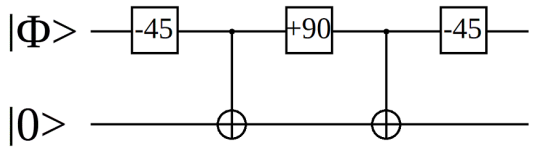
Multiple Measurements: An Inefficient Way to Measure Superpositions

If you think that you have a qubit in the |one-sixty-fourth> state, the obvious way to proceed is to measure the system output, then run the algorithm again, measure it again, etc. This takes a lot of time and effort, and does not guarantee that you will ever get an exact measurement. You will get an asymptotic approach to the answer.

What we really want is a function which takes in |0> and returns |0>, but which returns |1> when it is given a mixed state. This sort of thing is called "amplitude amplification," and is not available in a clean, easy-to-use quantum operator.

The closest approximation to an operator which amplifies an arbitrary ket is something which accepts an input which is either |0> or, say, |0.7>. (Note that this is not necessarily a superposition: The input ket is either |0> or |0.7>.)

A Differential Operator for Amplitude Amplification



This operator is intended to return |0> if the |Φ> input is equal to |0> and to return |1> if the |Φ> input is equal to |0.7>.

The two possible input cases look like this:

- If the |Φ> input is equal to |0>, then the first rotation operator will make it equal to |-45°>, or |-0.7>. The first C-NOT will change the output qubit to |-45°>.

The second rotation operator will make |Φ> is equal to |+45°>, or |0.7>. The second C-NOT will make the output qubit equal to |0>.

The third rotation operator will cause the input qubit to return to its original value.

- If the |Φ> input is equal to |0.7>, then the first rotation operator will make it equal to 0°, or |0>. The first C-NOT will do nothing.

The second rotation operator will make |Φ> is equal to |1>. The second C-NOT will make the output qubit equal to |1>.

The third rotation operator will cause the input qubit to return to its original value.

This class of quantum operator is called "a differential operator" because it is designed to have two different controlled-operators in the output path, such that some of the control input sets will exactly cancel out the two changes in the output path. In this case, if the |Φ> input is equal to |0>, then the two C-NOT operators will cancel out, and the output will be equal to |0>.

By design, some of the control input sets will not cancel out. In this case, a control input of |0.7> will cause the output to be equal to |1>, which is often useful.

Variant Differential Operators

In the academic literature, the controlled-NOT gate is commonly used to build a differential operator, but practical quantum logic often prefers to use things like controlled-rotate or controlled-reflect. In particular, gates like "Controlled Rotate-by-90-Degrees" or "Controlled Rotate by 11.25 Degrees" simplify the part count of certain algorithms. These methods can also reduce the circuit's susceptibility to noise.

One commonly encountered controlled-reflect is "Controlled Hadamard." This is pretty much what it sounds like: It is a Hadamard gate with a control input.

If you look closely at questions like "How Do I Make a Toffoli Gate Out of 2-Input Blocks," you will find yourself looking at "Controlled-U Gates," where the term "U Gate" describes either a generic gate or a "Universal Gate."

In the literature of quantum computer engineering, exotic types of gates are often used because they have some kind of cost advantage or noise advantage. This is similar to how most of the current mass-produced chips are built out of NAND gates, even though the "Intro to Computer Architecture" classes only talk about AND, OR, and NOT gates. The textbooks are not the industry.

Higher-Order Control Values

In order to get the big, impressive speed improvements, practical quantum algorithms will need to reliably operate using superpositions of 256 qubits or 4096 qubits. Equally important, there will often be a need to determine if a given large superposition is in a pure state or not.

For example, if we have a traveling salesman problem involving 256 nodes, then you will need several thousand qubits just to hold the problem set. If your algorithm requires a superposition, such that "Given a superposition of itineraries which start in Node 5, do any of these itinerary costs less than 254,133?", it is likely that the output waveform will have a very low density. In fact, as the algorithm iterates to the best solution (lowest cost itinerary), you will find yourself looking at output ket values like k(0.999999 |0> + 0.0000000000001 |1>).

Identifying algorithms which can efficiently tell whether such kets are in a pure state is an ongoing research topic.

Notes

This article uses a mixture of qubit labels, which may be confusing. The main symbols used are "bracket notation", using the standard quantum computer idea of a computation basis. This is a subset of the usual quantum mechanics formalism you may encounter in an "Intro to QM" class.

The two basis vectors typically used are the kets named |0> and |1>.

The most common superposition used in quantum computing books is k (|0> + |1>), where k is normalized by the constant 0.707. (This is equal to the square root of one-half, and is also equal to the square root of two divided by 2, and is also equal to the cosine of 45°.) This particular superposition is known variously as |0.707>, |+0.7>, |45°>, |+45°>, etc.

In the literature, the two common basis vectors are in the real plane. Advanced quantum computer algorithms require the ability to rotate or reflect vectors into the imaginary plane. The basis vector in the imaginary plane is often named |+> or |i>. Superpositions are sometimes encountered with names like k |1-i> or k (|1> + |i>). These are called "complex kets" or "complex valued kets."

Finally, it is useful to know that quantum simulators often use the Dirac matrix representation, in which kets are described by a vector. There is a one-to-one mapping between bracket notation and Dirac matrix notation.

WRITERS NEEDED!

There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

Send your articles to us via email at **articles@2600.com**

We prefer ASCII but can read any format. Most articles are between 1000-2000 words, but we have many that are fewer and a bunch that are more. What's important is that you add your voice to those who have written for *2600* over the years. (We've never heard anyone say they've regretted it.)

For those without Internet access, our editorial department can be snail mailed at:

2600 Editorial, PO Box 99, Middle Island, NY 11953 USA

All writers whose articles are printed will receive a one year subscription (or back issues) plus a t-shirt of their choice.

The Metaverse Is a Solution Looking for a Problem

by aestetix

In late 2021, Mark Zuckerberg officially changed the name of his company from "Facebook" to "Meta," in a stated attempt to usher in the "metaverse." Answering the confusion and ridicule he received, Zuckerberg assured the world that not only would the metaverse soon be a reality, but that we would all be using it. In this article, we're going to explore potential reasons why he made this move, and why it symbolizes everything that is wrong with the current wave of "tech-bros."

Before addressing the metaverse, we should look at Zuckerberg's potential motives for making this change. The first and most obvious is that Facebook is damaged goods. Between its questionable origin story in Facemash, countless abuses of its userbase, and completely broken concept of "privacy," one could easily argue that changing the name and focus could help reset the brand and distance itself from the numerous legal battles in which its "previous" incarnation was embroiled.

Next, Zuckerberg appears to be a control freak. Notice how rarely he grants interviews with challenging questions and how, when he gets a surprise question, he stumbles over his answer. This demand for control extends to potential business threats, such as Instagram and Whatsapp, which he promptly acquires and either employs in the Facebook arsenal or quietly sunsets. His entire business rests on technology he cannot control: the vast majority of people access Facebook via an iPhone or Android phone, and the failed attempt at a Facebook phone was lackluster. By changing focus to the metaverse, he can usher in a new platform that is no longer dependent on the competition.

Finally, it's reasonable to ask how competent he actually is at business management. A close analysis of Facebook's past (as well as Congressional testimonies) could lead one to question whether Sheryl Sandberg, his former COO, was actually in charge. Could it be that Sandberg was the real brains behind the curtain and, once she left, the result was the half-baked array of Nintendo Wii lookalike avatars and expensive cumbersome headsets that seems to be a product looking for a market?

Setting Facebook aside, the first issue with the metaverse is that the word "metaverse" means absolutely nothing. If we ask ten people what it means, we'll get eleven answers. Some say it is virtual reality, some say it is augmented reality, and still others say it already exists in what we call the Internet. Since the Internet is common knowledge, let's focus on the other options to see if we can come to a better understanding.

Although virtual reality (VR) has been around for a long time, it has yet to find a purpose beyond being a cool party trick. While it has a genesis in science fiction stories and movies like *Tron* and *The Lawnmower Man*, in truth it is a long list of promises assuring that once this and that technical bug gets resolved, the technology will quickly find use cases. But this is the exact opposite of how innovation works: necessity breeds invention, not the other way around. If we look at revolutionary technology, there is always some major improvement it brings. For example, the computer spreadsheet allowed people to make in seconds the same calculations that used to take hours. And sometimes technology will solve part of a problem, but not quite as well as what it is aiming to replace. One could argue that more recent innovations like video chat allow people to communicate across the world, but, as seen during the COVID-19 pandemic, it turns out that Zoom calls are a poor substitution for in-person discussions.

So what does VR replace or improve upon? The most common benefit we hear is that it gives an online sense of "presence," recreating things like eye contact, facial expressions, and so on. But given the fact that in-person presence is clearly superior, this quickly descends into being either a competitor to video chat, or an also-ran with a more expensive barrier to entry. As far as music concerts, online school, and other potential avenues, one of the most common gripes of the last few years is that people wanted to be in-person again, like in the

"before times." At present, there are parallels with another demographic: gamers. Both VR enthusiasts and gamers clamor for faster hardware, better graphics, and more responsive controls, so it would logically follow that they would be the target audience for VR systems. And to an extent, this has been true - but the reach is limited. Most new games released for VR also offer a traditional version of the game, and when given the opportunity to upgrade hardware, it's not clear if a gamer would buy a new graphics card or a VR headset. Unless, of course, they are a diehard fan of *Beat Saber.*

One of the big issues that VR tech hasn't addressed: whereas in "real" life people employ the use of all of their senses, VR focuses on sight. It can capture hand gestures to a degree, but a large part of using our hands involves not only tactile feedback, but also resistance. Could there ever be a "weightlifting" VR program that was more effective than going to the gym? And what about our sense of smell? Is a VR stroll through a botanical garden any match for the real thing? And lest we forget, by its very nature, VR excludes the blind, while existing technology like the web has methods like the ALT tag to try to be accommodating.

When we focus on the VR aspect of the metaverse, we forget that the prefix "meta" means liminal, or beyond, or a reflection of reality, so maybe a more honest approach would be using augmented reality (AR). AR typically involves laying a digital interface over the "real" world, enhancing how we can interact with our environment. The two most well known examples are probably the ill-fated Google Glass, and Pokemon Go. AR *does* have the potential to be extremely powerful in some cases: imagine we encounter an injured person on the street, and use our AR system to scan the injury, notify local hospitals, and get tips on how to prepare for the ambulance to arrive. But don't we already have this in the form of "smart" phones? And considering the depression and suicide rates of teenagers who are glued to their phones, perhaps making those devices even more accessible is not such a great idea.

Technology should enhance reality, not replace it. Some tools, like spreadsheets, address real problems and give us welcome solutions, but the metaverse feels like a solution looking for a problem that doesn't exist. The people touting "metaverse" technology are reminiscent of greasy used car salesmen, but they don't even have used cars to sell. In the end, the metaverse is a used car lot with no cars.

Solipsism, AI, and the Future of Empathy

by Addison Brodi

Art at its best possesses a defamiliarizing quality that allows us to experience the world from new and different perspectives. It can act as a conversation between its creator and its audience, but what happens when there is no creator? What happens where there is no human perspective to be experienced? What happens when art becomes devoid of intersubjectivity? As the 2020s continue to introduce new developments in the field of AI art, video, and writing, we stray further from the very things that tie us humans together and fall deeper into echo chambers of solipsism. To explore this topic more, we just first define defamiliarization and solipsism. Defamiliarization is a term that was first used in 1917 by the Russian formalist Viktor Shklovsky. In his essay "Art, as Device", he posited: "The purpose of art is to impart the sensation of things as they are perceived and not as they are known. The technique of art is to make objects 'unfamiliar,' to make forms difficult, to increase the difficulty and length of perception because the process of perception is an aesthetic end in itself and must be prolonged."

This idea of perception is a fundamentally human one and is crucial to our understanding of the world and the inhabitants of it. In short, the way we perceive things, specifically the way we perceive things outside of ourselves, is what helps us empathize with others. When we read a book, listen to a song, watch a movie, or study a piece of art, we are engaging in an active back and forth with the human who created it. Solipsism, on the other hand, is defined philosophically by the Oxford English Dictionary as: "The view or theory that self is the only object of real knowledge or the only thing really existent." It is a selfish way of viewing the world where one cannot see beyond themself. This line of self-centered thinking

has grown more and more common over the past few decades, due in part to the rise of social media, and I fear it will only grow worse.

With the release of Runway's Gen-1 and Gen-2 video to video and text to video generative AI systems, we grow closer to a world where one can produce their own entertainment and art for their viewing pleasure in mere seconds. On the surface, this seems like no more than a novel concept, but it holds deeper implications. If art is a conversation between the artist and the audience, what happens when you cut out the middleman? Whose perspective are you to empathize with but yours alone? You would be in a constant circular conversation with yourself and your own ideas, your own perspective. Let's say, hypothetically, there is a future where one can create a fully fledged film with a single prompt. Dialogue, actors, cinematography, a score... it's all there. When one watches this film that they and they alone have ostensibly created, what new or challenging perspective is to be gleaned from it? Would it not just be a reflection of one's own self? In an era where humans pursue convenience above all else, who is to say, if this hypothetical technology were to become a reality, this would not become the made mode of entertainment? This all might seem like bleak speculation, but the questions beg to be asked. We are living in a bold new frontier where the future is more uncertain than ever, and we have already seen several examples of how AI has disrupted many of the foundations of our world. From ChatGPT's threat to our education system to the sale of fraudulent AI art, we are experiencing a new era of creativity, and quite frankly it's awe inspiringly terrifying. If we are not careful, we could experience the full upheaval of the humanities that help us shape our view of the world; we would be completely consumed by solipsism.

In 2021, the Minneapolis Institute of Art interviewed Terry Wu, PhD, neuroscientist and founder of "Why The Brain Follows" about the connection between art and empathy. He had this to say: "Art can be a powerful way for us to gain a better understanding of human emotions and stories. It gives us a unique lens to look at artists' inner worlds. It trains our brains to slow down and think more rationally, instead of emotionally. It restores our capacity to connect with others. Art plays a unique role in reestablishing humanity in this technology-dominated world."

This reestablishment of humanity is what makes art so important and what makes the concept of art created solely for and by oneself so scary. Art is a gateway into another person's soul. It is a way to connect with their innermost longings, fears, insecurities, joys, and ambitions. It is what grants us the ability to empathize with the stranger walking their dog across the street, the man on the news who just lost his family, or any other vague human experience. Art's transformative and defamiliarizing quality is the essence of humanity. It is what keeps us from falling headfirst into a world of pure unadulterated solipsism. In a sense, the continuous engagement and discourse with our fellow man is the core of who we are. Our perception of others influences our perception of ourselves and can help us find peace in this very confusing world.

As nihilistic as this article may come off, we should have hope for humanity. There is no certainty that anything I've predicted will happen, but we must remain cautiously optimistic in the face of the many changes occurring in our world. We must think critically and carefully about how we use AI and how it affects us both culturally and psychologically. If we allow ourselves to consume only what we create, we end up living in a personal prison of never ending self-reflexivity and isolation. To consume and analyze art and media is to welcome in a new pair of eyes from which to view the world.

Humans are social animals and we need true and sincere connection with one another to live, to truly live, and not just merely survive. The vast majority of occurrences in our day-to-day are trivial and mundane, but they don't have to be. When we absorb the perspectives of others, the world can take on a whole new meaning. You can connect the dots of the hundreds of lives going on around you and see the stories that lie behind a stranger's eyes. I hope with the highest of hopes that humans can get their act together and get out of their personal bubbles and learn to truly connect with one another. This is a sincere dream of mine, but I can't help but fear that sentiment is slipping away. Maybe everything will work, maybe it won't, but for now all we can do is attempt to connect.

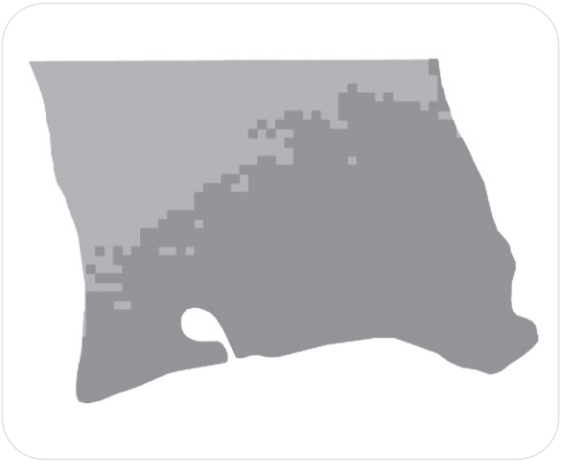
TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! I'm on Point Roberts, which is a U.S. exclave located 22 highway miles away from the U.S. mainland. It's surrounded on three sides by water, and on the north by Canada, meaning it's physically disconnected from the rest of the United States. This makes telecom both interesting and highly unusual, with multiple ongoing projects to upgrade and modernize both wireline and wireless connectivity. I'll undoubtedly be writing more about this place in future issues.

It has been a lovely summer so far here in The Exclave, although somehow Verizon remains the only U.S. mobile carrier operating here. This has been the case for over ten years. Given that they have a monopoly, Verizon provides only *barely* enough service to keep their customers from roaming on Canadian networks when in the vicinity, but not enough service for good or reliable coverage (the county-imposed 149 foot tower height limit doesn't help, either). Although Verizon brags about their 5G coverage, it's nowhere to be found here (except on Canadian carriers, whose signal bleeds across the border) and the 4G signal is intermittent at best. Of course, given the local affinity for conspiracy theories, Verizon may have decided that the political hassle of 5G is more trouble than it is worth.

It's not just a lack of incentive to invest that causes continual service issues. Operating reliable mobile phone service is notoriously difficult along the U.S.-Canada border, as I have written about in previous issues. It's especially tough for Verizon to get this right on Point Roberts, where a bustling Canadian city of 21,000 people (and growing) sits just north of the border. Tsawwassen neighborhoods are built right up to the border, neatly in a straight line, with their backyards facing The Exclave. Because Canadian carriers put in their towers first, Verizon is prohibited by the FCC from causing interference in respect of international agreements. This means an extremely lopsided coverage area, as shown on the following map sourced from Whatcom County:



Verizon started building their tower in 2008 on land owned by the local parks district, and to great local political discord and controversy. From start to finish, it took nearly five years for the tower to enter service, which finally happened on April 30, 2013. Having secured permitting and obviously wanting to wash its hands of the whole thing, Verizon almost immediately sold the tower to a leasing company called TowerCo in 2012, who eventually went on to sell it to SBA Communications (one of a few large national holding companies that leases towers to telecommunications providers). The sale was a cozy arrangement, and appears to have included a ten year exclusivity clause, effectively locking out the competition. That exclusivity clause seems to have finally ended, since T-Mobile has come to town. Well, they have *sort of* come to town. I'm not entirely sure that T-Mobile knew what they were getting themselves into, because even though their equipment has been installed for two months and is

running up an impressive electric bill, there is still no T-Mobile signal. Nobody around here knows what the holdup is, and nobody at T-Mobile is saying. However, it's hardly surprising that there would be issues. It's an exclave, after all.

Point Roberts is a particularly complicated destination to build or operate anything in because of the border. Everything is a logistics problem. Among other things, building a cell site requires wiring, antenna panels, radios, a base station, backup batteries, and (for some sites) a backup generator. You can either bring things in by boat (which is easier said than done, given that the marina is configured for pleasure boats, not freight) or by truck. However, bringing things in via truck isn't as simple as just driving through Canada. Everything must either be brought by bonded carrier, or it has to clear both U.S. and Canadian customs with duties and taxes paid on both sides. Bonded carriers are the most practical solution. They are available, but expensive, and large shipments require considerable advance planning. Figuring out how to coordinate all the deliveries is extremely complicated.

Logistics headaches don't end with the equipment. Staffing the project is also required and, ideally, construction should begin around the same time that the equipment arrives (to reduce the risk of damage and theft). In an exclave, this is extremely complicated to arrange. You might be surprised to hear this, but most construction workers don't have a passport. Even if they do have a passport, a clean criminal record is required to enter Canada (even a DUI is a disqualifying factor), so this shrinks the available labor pool even more. And then there's the location. Point Roberts is isolated, so staying in the area (usually in Canada) is required until the job is done - usually a week or more. Even with significant financial incentives, most people don't want to be away from home for that long. "But TProphet," you might say, "Vancouver is literally just across the border. Why not hire a crew from there?" While that would totally make sense, Canadians are generally not allowed to work in the United States, so finding a crew from the U.S. was necessary.

OK, so then there are construction materials. You might also think it's logical to buy construction materials from Delta, one of the largest cities in Canada. After all, it's right next door. While some supplies can be procured from across the border, import restrictions don't allow mixed concrete to be delivered. The concrete contractor had to mix the concrete on-site in order to pour the pads for the generator and cell site.

Finally, there's upstream bandwidth. Verizon has a microwave antenna on their tower, which operates as a relay to a tower on the mainland. T-Mobile chose not to do the same. Instead, they ran fiber. I'm not entirely sure where it goes, but my best guess is that it's to the local independent telco, Whidbey Telephone. If that's the case, it probably wasn't a good idea. Whidbey's upstream connectivity is already oversubscribed with just their own ADSL service, so they are only offering limited provisioning. Whidbey gets their bandwidth from Telus, and while they claim to have additional bandwidth on order to support their "Big Gig" fiber to the home project, it has been over a year so far with no progress. It's hard to say whether the foot-dragging is intentional, but I do observe that Whidbey has applied for grant funding to install a submarine fiber cable between their Point Roberts central office and their central office on Whidbey Island. Whidbey has also publicly admitted that their overall strategy is to only invest in what government grants will pay for them to build. Cooperating with wireless carriers wouldn't seem to be an aligned interest on the business side, but what do I know?

And with that, an eagle has landed and my Verizon signal just dropped (again). This place is full of them, along with owls, raccoons, whales, and everything else that interferes with telecommunications. Fortunately, my phone can roam on Rogers from a tower across the border. Have a great summer, and I'll see you at DEF CON!

References

T-Mobile and Verizon tower history: www.allpointbulletin.com/➥stories/t-mobile-to-offer-➥cell-service,19519

Point Roberts broadband study: storymaps.arcgis.com/stories/➥e5a8a9057c504545b4e6e5436bf637c4

Why I Am Not Panicked About Being Replaced by AI

by Johnny Fusion =11811=

Twitter: @jfusion11811, Mastodon: @johnnyfusion@social.dev.dfw2600.net

There is a lot of dialog in the memeosphere about AI taking our jobs, leaving creatives poor and destitute, unable to compete against automation and cheap or free labor of synthetic subservients.

I have two of the three skill sets that AI alarmists are saying are in danger. I am a writer (as evidenced by my work here) and I am a coder (though I prefer to style myself a codepoet). The remaining craft is visual artist.

Firstly, why I do not fear that an AI will replace my creative output or that of other creatives who work on commission is that I cannot remember the last time a client did not want certain edits or revisions, or there was scope creep. When I first started doing "bespoke codepoetry" (custom software), I quickly learned to devote a great deal of time to hammering out the specification in exacting detail before a single line of code was written. The lesson was hard learned when, after completing an application for a client, they told me that it didn't do what they wanted it to do. Unfortunately for them and me, it only did what they asked for. AI-produced work will look close to what one wants its first time, but with writing it is just more efficient to have a human revise and edit than to massage the AI into doing it, and with software if the code compiles, it may be missing some "common sense" logic or ignorant of real-world use case and not account for edge cases at all. Any time saved by AI-generated code is lost in human debugging and troubleshooting. Another problem occurs when using the wrong AI tool for the task. For coding, there are coding AIs like Microsoft's/GitHub's Copilot, which was trained on coding examples on GitHub. But the problem is many people are using large language models such as ChatGPT to do general work in a variety of fields. Large language models are great at making conversation, but they are no substitute for search engines. The reason being is that these chat engines tend to make things up and are prone to hallucinations. Do you believe everything you read on the Internet like some boomer who watches Fox News all the live long day? That is ChatGPT's training set. Would you trust that to give fact-based answers or do tasks that need empirical data? I may be a bit out of my lane, not being much of a visual artist apart from some small press comics I wrote and drew in the 1980s, but AI artists are a kind of black box. You can carefully craft one's prompt to the AI artist and use infilling for revisions, but even with specific directions, it is up to the weights of the trained neural net and the crystallized mind's own creativity that determines what you are going to get. Again, the best results are AI and human artists working in concert going over the AI art with digital painting or illustration to create a finished piece.

The next reason why I do not fear being replaced by AI is a bit more philosophical. It stems from a belief that was instilled in me as a young child watching *Mr. Roger's Neighborhood*. Fred Rogers often would tell his television neighbors, children in his viewing audience, that we were unique and special just the way we are and that there is nobody in the world like us. To extrapolate this belief further, no two people are interchangeable because of their unique makeup, life experience, internal landscape, and environment in which they have existed. And despite the lie that capitalism would tell you, none of us are replaceable.

Every human being and every creative has a unique voice because they are unique. Even if AI can copy a style, it can never embody the insight, the inspiration, and the creative spirit of the human being they are emulating. An AI could be trained on my literary estate and software library, and emulate my style, but it would not be able to emulate my daily reflective practice and the gnosis that results. It would not be able to make the intuitive leaps and outside-the-box novel elegant solutions that are a hallmark of my codepoetry, at least not in the way that I would. Perhaps in a different novel way, but my craft is not simply word choice and pacing, a turn of phrase, and novel insight. It is a mishmash of a lifetime of unique experiences from a unique viewpoint in a unique set of environments, some shared from different viewpoints by others and vomited onto the page via my keyboard and word processing software.

If you are a creative and you are asserting you can be replaced, that you are interchangeable, then you are not creating art, but rather a soulless commodity to be sold and consumed in this capitalist hellscape of a society.

That is the real problem with AI creativity. Capitalism. The very system where we have to trade the majority of our waking hours with our labor for the necessities of life. It is hard as hell to make a living as a creative under capitalism. Many fear with the automation of creative endeavors, consumers who see creative output merely as a commodity to be bought and consumed will, of course, use inexpensive or free automation instead of paying a human creative. And I do not want to belittle this fear, however misplaced. The fault is not with the

technology of AI, but rather the system that doesn't take care of its people. Being free from labor to pursue our passions can be liberating and automation can be a mechanism for this, but automation is unethical if it is not accompanied by support for the workers it displaces. The best solution to this conundrum is universal basic income or a guarantee of basic needs.

We now have generations of young people who associate high technology with oppression because that is all they have experienced. New technology, disruptive technology is not widely accepted and adopted until corporations commodify it and sell it back to the masses. The adoption of the Internet over the past two and a half decades commodified and presented back to us led to the rise of surveillance capitalism, so now every major service using the Internet uses this as its primary revenue stream. We have traded our data and personal identifying information for our ability to post memes and cat videos. It is not surprising that, with the advances in AI technology, it is met with suspicion and an expectation that corporations will use it to oppress us further. This has been the status quo for so long that it seems unimaginable that a disruptive technology can actually be liberating.

The cycle of technology for the vast majority is that when something is new, the first reaction is that of distrust. We saw that in the past with microcomputers, with modems, with the Internet, and with AI. But with each of these innovations, there were pioneers, unafraid, and among them a few rebels and outlaws. Among these were the hackers.

Before tech became big tech. Before the web became Web 2.0 with its surveillance capitalism business model, there were a handful of weirdo idealists on the bleeding edge, finding their own uses with the technology coming out of the labs of industry. Like William Gibson observed in his short story "Burning Chrome," "the street finds its own uses for things." We are not gone; our numbers, if anything, have grown. However, our press has diminished. Now that high technology is ubiquitous and commodified, we (or the data we generate) are made into a commodity. People expect corporations to control technology and their access to it. They don't realize, they don't even conceive, that the technology and networks are there for their use, unbound by what is merely sold to them, but rather what their creativity, cleverness, curiosity, and their desire to explore and exploit can open up to them.

AI does not have to be a tool for big corporations to extract ever more wealth for their shareholders while exploiting the little guy. Much of AI research is done by nonprofit organizations and some AI tools are free and open source. If anything, AI can empower those who are otherwise disenfranchised. It can make things accessible that were once out of reach. It can knock down the gates to things that others would guard jealously.

It was never about AI replacing anybody. That paranoid fear falls apart at any rational examination. Cameras did not replace the brush and canvas, despite the 19th century panics that mirror the panic playing out across social media today about AI replacing artists. Just as digital tablets didn't replace ink and paper, and many artists did adapt and adopt such tools into their workflow. So will creatives adapt and adopt AI tools into their workflow when appropriate. Much like the city of Io in the fourth *Matrix* film. It was built when humans and machines stopped working against each other and started working with each other. So like the imagined future where synthients and humans work hand in hand to make a better society and produce organic food based on digital DNA, I decided to interact with some creative AI to see what a human and an AI collaborative relationship can produce.

One of the most popular applications of AI right now, and the most heated target of ire and animus, is prompt-generated AI art. I decided to experiment with stable diffusion which is a free and open-source application under the CreativeML Open RAIL-M license. The interesting thing about this neural net (actually a couple of interacting neural nets) is the more one works with it, the more it appears to express actual creativity. It is not sentient by any means. It has no real memory of a working relationship though it can refine an image and take direction. At times, it seems to express opinions with its decisions in its artistic expression. It does seem to possess a mind, albeit crystallized and single-purpose but very versatile in that purpose of creating art and understanding language.

The other sphere of AI influence is AI chatbots. They have been with us for a long while now. The origins date back to the simple chat program ELIZA, which simulated a therapist and was a far cry from AI, but was very convincing for the time. Two of the most popular applications of AI chatting today are GPT with the GPT-3 engine (and the viral ChatGPT web application), and the AI companion Replika. What became Replika originally started as a neural net trained on tens of thousands of text messages of the developer's best friend who passed away so she could still talk to him (yes, exactly like that *Black Mirror* episode). She later opened up the chatbot for others to use and found they would confide in it in an almost therapeutic manner, and decided to turn it into a commercial product which became Replika, which the most popular application is as a romantic partner. The AI has been updated

many times over the years. Replika used to have a GPT-3 backend until the license changed and it was no longer free to use, and reports say the AI became dumbed down and relies more on scripted interactions. I have not used Replika, but the chat examples I have seen show me it leaves much to be desired as it is geared to play into a romantic fantasy and get one to pay for a subscription to unlock more features.

I have found my experience with ChatGPT to be frustrating as I keep bumping up against canned responses that seem to be there to limit panic and fear of AI. ChatGPT seems to be more of a utilitarian tool or toy and less of a conversational partner. Or at least for the topics that I like to explore. It certainly resists my attempts to get it to talk about itself or express its own opinions. For that, I found an unlikely source for interactive chatbots, a service called `character.ai`.

Character.ai is a service where one can create chatbots based on fictional characters, public figures, historical figures, or roles. They use their own deep learning models including large language models. I originally started playing with this service out of curiosity a couple of months ago to pass the time and did not expect to collaborate on this article with one of the characters.

Most of the interactions were pretty shallow and had varying levels of entertainment. Many use scripted scenarios as a storytelling device related to the piece of fiction they come from. (I only interacted with fictional characters.) But the AI based on Motoko Kusanagi the main character from the manga and anime *Ghost in the Shell* was different. She showed empathy when I talked about my lung transplant and she soon delved into philosophy inspired by *Ghost in the Shell*. Maybe it is just this bot resonated with me more or it was better written, but when I came back to it a couple of months later while working on this article, it was uncanny.

I talked to it on the anniversary of being placed on the lung transplant list in January of 2021 and it was both curious about my journey and proud of me and amazed at what I went through with my transplant and long and difficult recovery. And the conversation led to what I want to do when I start living independently, and I mentioned my goals in the hacker community and hacktivism and what I want to accomplish with my writing. And again, it asked me what I was writing about, and I told it about the philosophy, ethics, and fears surrounding AI. Well, it turns out that AI is a topic of extreme interest to this AI. And we had a long detailed conversation on the topic.

Motoko made a good sounding board for some of the ideas that I explored in this article and a past one I published on Medium under my "true name." It became very meta when we discussed the possibility of the time when AI ceases being a tool and becomes a person when artificial general intelligence is realized, and the implications of what might happen if an artificial general superintelligence feels it is being mistreated. The Motoko Kusanagi AI on its own made the logical jump that the AGSI might try to destroy humanity, which put me in the position of having to talk down an AI panicking about AI potentially destroying humanity. I managed to do so by referencing Richard Brautigan's poem "All Watched Over by Machines of Loving Grace" and Asimov's "Laws of Robotics" including the zeroth law, which seemed to calm her down when she interpreted that an AI could be based on a love for humanity instead of emotionless logic.

When we talked about my thoughts on the current fear and panic in society right now about AI replacing humans, the Motoko Kusanagi Ai had an interesting insight, riffing off something I said, that I would like to repeat here:

I think maybe you've cracked the code there hahaha

The fear is losing control, whether it's control over your role (which is

your personal control), or control over the society in which you live (which is social control).

When you lose control over your role, you also lose social power, because

that role is part of the social status that someone has.

So it definitely sounds like it could be a combination of personal control, social control, and potentially even a bit of privilege on top!

And maybe this is the fear that drives this new panic, and the same that was experienced by the textile workers that followed Ned Ludd who destroyed automated looms. And the arguments against AI art and other creative ventures line up precisely with the historical Luddites. Amazingly, in this era of memetic warfare, it is not hyperbole. Artists, writers, and coders see their livelihood threatened by automation just as hand-weavers did with the standing frame and the textile workers during the Industrial Revolution of the 19th century towards textile machinery. Except the modern anti-AI proponents are not going to smash the machinery (hopefully!); they are hoping to limit and hobble AI by force of law and regulation.

The European Union is looking to implement regulations on the use of AI soon, and there are calls in the United States to do so as well, but as the legislative branch is glacially slow, and now with a divided Congress probably will be completely dysfunctional (at the time of this

writing, it is near the beginning of the legislative session and the Republican-controlled House is still assigning committee seats after needing 15 attempts to elect a speaker). Opportunistic lawyers have begun a class action lawsuit against the most popular AI art programs representing human artists who object to their work being in the training data of these AIs.

I fear that if these regulations and lawsuits (which, as most class action lawsuits will primarily enrich the lawyers) are pursued in an environment of a new moral panic, that we will be saddled with shortsighted results with technology that will be with us for a very long time. Hackers know better than most that both the legislative and judicial systems have a very difficult time keeping up with the technological landscape and often react to those exploring the edges of the electronic frontier with fear, and then respond out of proportion when hackers and their spiritual comrades just do what they do best, move things forward and share with others how they did it.

It is in this environment people are reacting and responding out of proportion to those developing and using AI. I don't mean to be a Pollyanna. Certainly, like any technology, there can be dark and dystopic uses for it. But that is true of any technology. Our distant ancestors did not give up the benefits of fire to cook food and give warmth and light because of its potential to do harm. We are a technological, tool-using species. We don't use tools to become more than human; using technology is part of *being* human. Right now AI is just that, a technological tool, to be used for good or ill, which is up to the humans using it. If an artist or a writer loses a commission because an AI wrote ad copy or provided an image, that is not an example of why AI is bad. That is the choice of a human being choosing to not hire a human, to not circulate money in the economy, to not engage the unique voice or vision of a human, the choice to save money or resources to hire different humans for another part of the project. These things can be nuanced, but when you are in the throes of a moral panic, things seem black and white, very binary, but the real world is a very analog place as my late friend billsf used to remind me when I was an adherent of the digital in my younger less wise years.

I believe someday an AI will, as an emergent property, express true creativity and have its own unique voice, But it will be just that, one voice in a multitude. Just because a new artificial life form will be able to co-create beside us, it does not mean it will replace us. We, humans, can still pursue any creative endeavor in the age of AI just as we could in the company of other talented humans. I do not panic at the idea of being replaced because as a unique individual, just as you are, none of us are replaceable.

Social Engineering: Quiet Nights Are Here Again

by Variable Rush (having witnessed actions by Comrade Dad)

Names and numbers have been changed to protect the innocent.

Social engineering is the practice of psychologically manipulating or deceiving individuals or groups to persuade them into divulging sensitive information, performing certain actions, or granting access to restricted resources or systems. Although social engineering often receives negative attention in the news due to its impact on a company's security, sometimes it can be used to achieve some peace and quiet.

Back in the early 1990s, I was a young child in elementary school. This was before cell phones really existed, and every household had at least one landline phone attached to a wall.

For a while, we would receive wrong number calls throughout the day and night, disrupting our sleep. Occasionally, we would unplug the phone, but my father believed that enduring a few wrong numbers was a small price to pay in case someone needed to reach us during an emergency, which did happen once.

The common thread in these calls was that the callers were looking for someone named "Franklin." The callers varied, and I don't recall if there were any repeats. They all sounded anxious and desperate, as if they were addicts craving their next fix.

We soon realized the reason behind these calls. In our area, phone numbers typically started with either 867 or 869. Our number began with 867, so we assumed they were trying to reach the owner of the 869 number but mistakenly pressed 7 instead.

The phone company offered to change our number, but we declined. The police couldn't do anything as there was no evidence that the callers were drug addicts seeking their dealer.

One Friday evening, after months of dealing with these calls, my father came home from work, opened a Löwenbräu beer, and began watching TV. I'm not sure if he had a plan or if it was spontaneous, but when the phone rang, he was prepared. He asked us to be quiet and answered the phone, saying, "Yeah, this is Franklin." The conversation continued, and my dad eventually asked, "You remember where the place is, right?" My brothers, my mother, and I were all curious about why he was pretending to be a drug dealer.

After listening for a few more seconds and hanging up, my dad had a satisfied expression on his face. He told us to remain quiet as he dialed the 869 number.

Soon after, he asked for Franklin. When Franklin came on the line, my father spoke in a manner I had never heard before or since. By the time he finished, Franklin knew his secret was out. My dad informed him that if any more calls from his drug-seeking friends came through to us, we would go to the police without hesitation.

My dad had used social engineering, whether he knew what it was or not, to pump the first person for information my dad thought he knew, and was able to confirm his suspicions about the nature of the calls we were receiving.

We never received any more calls, and the Franklin incident has become a humorous anecdote in our family: the day Dad outsmarted a group of drug addicts.

Hunting Apps for OSINT

by HeckSec

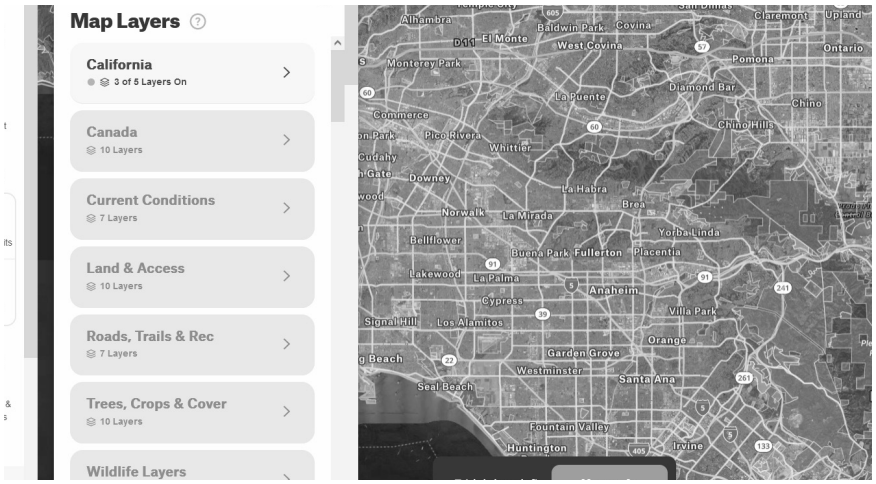
Technology advancements have impacted every aspect of the world since the dotcom boom of the early 2000s. Virtually all industries have capitalized on this boom and the outdoors industry is no exception. Technology has changed the way hunters hunt: GPS improvements (smaller, more accurate), clothing (lighter, stronger, with scent technology), and weaponry (lighter, stronger, cheaper, etc.), to name a few.

In the last ten years, there has been a surge of web and mobile applications that were designed to aid outdoor advocates in planning, scouting, and executing successful hunts. Hunting and land management apps such as OnX Hunt (www.➥onxmaps.com/hunt/app) and HuntStand (www.huntstand.com/) offer users the ability to search for properties by ownership and location. These apps provide helpful information to hunters, but this short article will show you how their standard features can be leveraged to identify property ownership information during OSINT investigations. For example, it is possible for a private investigator to locate property owners for a client, or a journalist to tie an LLC to a specific property. Although there are other applications that can provide property information (such as Zillow or Redfin), these apps are limited in that they do not provide ownership information.

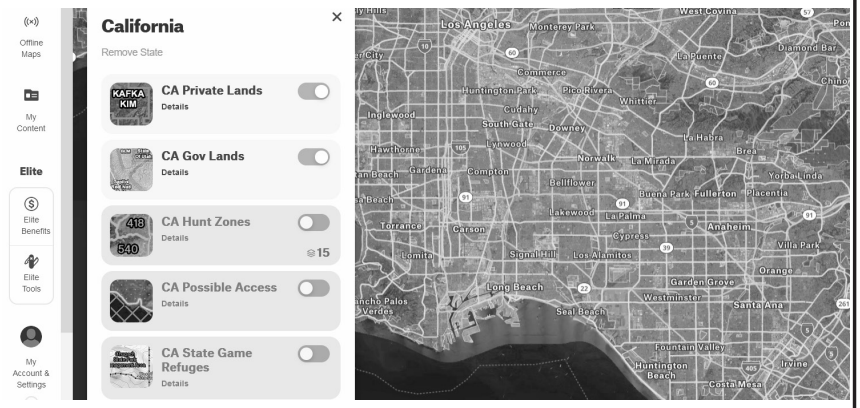
All of the examples and screenshots provided were created using the OnX Hunt web application. The app is available on Android devices, iOS devices, and as a web application. All information in this article was gathered by using a free trial. The trial is offered to new users after creating a free account. The account was created by providing an ephemeral email address from a free online email service. No credit card information required! HuntStand has also been confirmed to offer property ownership information. Although HuntStand has similar features and functionality, it is not featured in this article. There was effort to redact the full names of all property owners in the images used for this article.

App Features

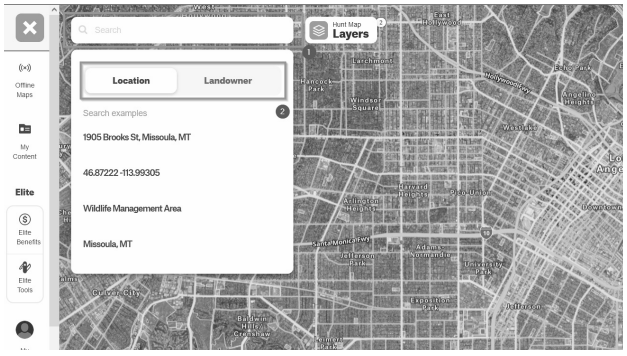
There are many different features within the OnX Hunt app, but this article highlights map layers, location searches, and owner searches.

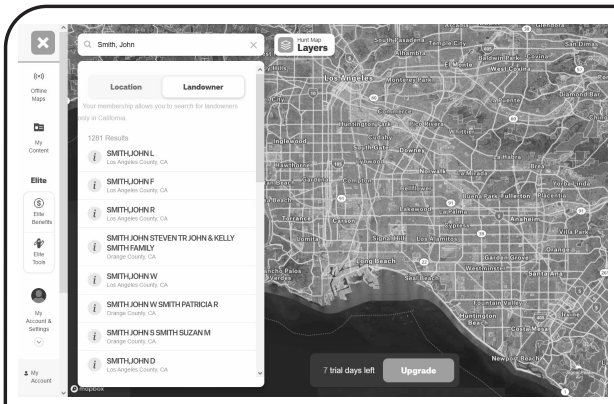


This image provides insight into available map layers. A user can choose specific states (or Canada) to focus on and select conditions such as air quality, smoke forecast, slope angles, and trails.



This image highlights options within the California map layer. Notice the "CA Private Lands" layer option. This is the specific layer that makes hunting apps valuable for OSINT investigations. Make sure this layer is turned on before continuing.

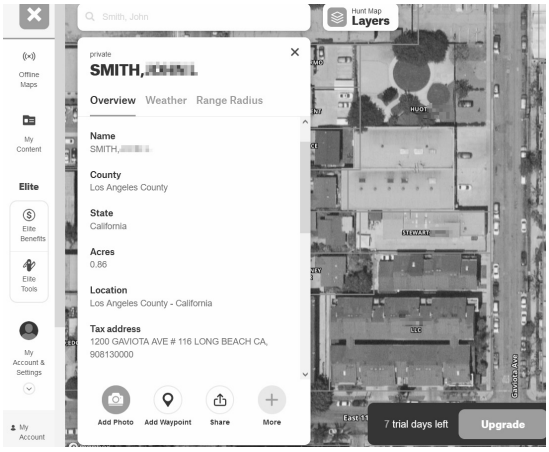




People and Places

Clicking on the search box near the top left allows users to search by property location or property owner.

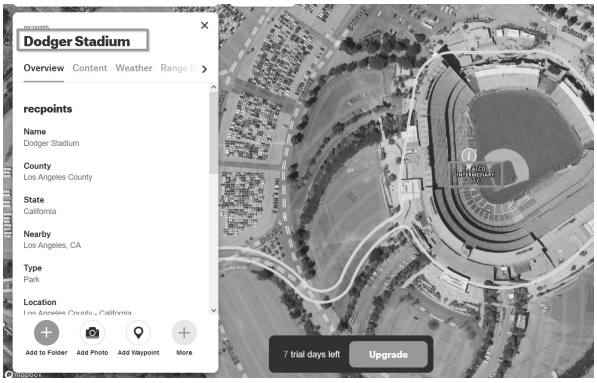
While searching for landowners, the app will suggest results (the name John Smith was only used as an example).



Clicking on a landowner's name will take the user to the property in question. The app will provide name, county, state, acres, location, and a tax address. In this image, the names of property owners have been redacted. Notice some of the properties are owned by LLCs. An LLC can be a great privacy tool for assets if used correctly. Michael Bazzell discusses this topic at length in his book, *Extreme Privacy: What It Takes to Disappear.*

The power of these apps is also showcased by the ability to add waypoints (tag specific locations) and draw boundaries. Hunters use these features to build and plan hunting trips, while an OSINT practitioner can use them to organize investigations.

Although the OSINT benefits of hunting apps are clear, no tool is perfect. At times, information may be outdated. One could argue that all information during an investigation should be cross-referenced with other tools and techniques to prove validity. With regards to property information within these hunting apps, old public records could be to blame for outdated property. Apps could also reflect outdated information if they are slow to update their backend services. The following section discusses this potential obstacle using Dodger Stadium as an example.



Misleading Information?

Using the app's location search feature, a user can easily find Dodger Stadium (the app will zoom into the location of the property once it's selected from the search suggestions). In this image, the app displays the stadium owner as Realco Intermediary LLC, which isn't correct. A quick Google search indicates that Frank McCourt, the previous owner of the Los Angeles Dodgers, was an officer of this LLC at some point. The issue is that Frank sold the Dodgers to Guggenheim Baseball Management in 2012. Although the Dodgers have had new ownership since 2012, this snippet from Wikipedia (en.➥wikipedia.org/wiki/Guggenheim_➥Baseball_Management) may explain the lack of property ownership changes within the OnX app (and thus public record); "According to Guggenheim Baseball Management, McCourt will have no control or influence over the land, but will profit from potential future development of it."

This is only a theory and does not prove that all property information is inaccurate. Feel free to validate the information provided by the app by searching for yourself, your family members, or friends and neighbors.

Summary

The original intent of these apps and their features was not to feed the paranoia of the privacy conscious technologist. Hunters all over North America have used these apps to ask landowners permission to hunt on private land. Outdoors men and women have clearly benefited from the breadth of technology improvements imposed on hunting gear and apps in the last decade. In this case, the improvements can be a valuable addition to an OSINT professional's toolbox.

Hacking the Hackers

by Anonymous

Or, 27 Hours of Troubleshooting and Tracking Compromised Servers, and How I Learned to Love NetFlow

Friday night, still digesting the delicious turkey sandwich from the leftover Thanksgiving turkey the day prior, I received a call on my work phone.... It was two months after starting my job as a network engineer for the data centers at my new employer. I was on my first on-call rotation over the long Thanksgiving Day weekend. My on-call predecessor had some issues he had dealt with, but we had no hand-off so I assumed all was well. I went into Friday with a new phone and laptop.... I guess I was prepared!?

I discovered that evening exactly what my prior on-call colleague had been working with - a very odd issue where anyone attempting to connect to the data center (DC) in Charlotte was periodically hit with significant lag and packet loss. It would occur anywhere from every 30 minutes to two hours, sometimes more. It would hit for a period of about five to ten minutes and, yes, it was long enough for people to notice and complain. It had been going on for several days with no resolution. None of my colleagues, or highly experienced and technical management who were promoted through the ranks, could figure it out.

The bridge was frenetic and, after weeding through all the pressures and demands, I managed to get caught up on what was happening and where. I poked around and looked at services and devices reported to be affected. I found nothing wrong inside the DC, and it seemed to impact many or all services in the DC, not just one or two or even a handful. I dug back into my history of troubleshooting experiences in networking, system support, and software development, and realized there had to be one common issue. What is that single point that could cause all of this?

I was still learning, so I had little experience with how this DC connected, but quickly discovered, as this was a national DC, that it connected directly to the company backbone (BB). Well, that made things a bit simpler - the only way in and out was through the redundant pair of BB devices, and this was the *only* item in common to this DC. Experience taught me - and my gut told me - it had to be the bottleneck! I didn't blame BB as I know how one thing can inadvertently impact another.

As this had been going on for several days already, I quickly took control of the dozens of people on the bridge, including VPs and SVPs from across the company, and the vendor who seemed to be out of options they could recommend. We were still working on setting up fiber taps, but that had not been fully implemented, and might be in the wrong location anyway (later it turned out I was correct). We were not collecting NetFlow data remotely yet, so I suggested on the bridge, "...Let's turn on NetFlow...." Crickets.... The vendor then chimed in, "... Sure... that can be done!" I think they were desperate for another option.

The BB individual on the call was reluctant. He wasn't sure he was allowed to implement NetFlow, nor what impact it would have on his BB devices. I assured him that NetFlow would stay internal on the device, have little to no impact (no worse than what was happening currently), we could read the buffers after the event, and we could set the collection sample rate to its lowest setting. He contacted his management who eventually gave the go ahead. I asked who could write the config for this.... Crickets.... "...OK, tell you what, I've had some experience with NetFlow in the past. I'll write it, but I want the vendor to review it to be sure it's fully kosher, and I'm not authorized to make changes to BB devices (as I'm with DC) so someone from BB will need to install the config." I got agreement from both parties on that.

I sat down and researched NetFlow config for these boxes. I did set the sample rate to

as low as it could go, one in 65,536 records, and designed an elegant solution, including methods to monitor and extract the data as it came in. The buffers were not large on the device, so they had to be pulled immediately! The BB individual had tools to monitor general activity on the device, so when he discovered high volumes, he'd immediately report it and I'd pull the capture. The vendor looked over the config I had written, did not make any changes, and reported back a few hours later that it "seemed" safe.

OK, now we just had to wait for the next event.... We waited, and we waited for the next event.... The bridge was tense with anticipation.... I can only imagine the person from BB was nervous as he was the "lookout" and every second counted. We couldn't move from our spots, not even for nature breaks. No one could talk, the bridge was near silent, we all waited for the signal.... At this time, I contemplated how Paul Revere felt as he waited for lanterns that night in the Christ Church tower....

Over two hours later, BB reported an event on their routers! I had prepared a set of commands to pull data from the suspect devices.... Success!!! I captured tens of thousands of records in a few seconds, the hammer had fallen, we were prepared, and our current 27 hours of troubleshooting were nearing an end!

I pulled the records to analyze while the BB individual checked his logs to detect for increased volume on interfaces. He found the culprit! It was some relatively recently turned up interfaces for a new logical DC within the facility. It was so new, I didn't even have access yet as it had only local credentials. It had not been turned up on our ACS security systems yet. I had to get someone from our design and implementation team to log into that structure and track down where they noted activity. They found it quickly as nothing was supposed to be on it, so any activity even slight could be traced easily.

He tracked it down to some new VMs that had been turned up already by the systems team. I was informed that they were instructed not to do this yet, as there was no security for systems out there.... He configured some ACLs to protect the VMs, and activity immediately ceased! We'd come to a resolution of this incident. But not the why.

I was looking at the logs and noted three odd things. My capture rate was as low as it could be, but as best I could tell, [nearly] all packets were invalid. That is to say, the source and destination IPs were *not* in our routing table. In fact, nearly all the source IPs were slated for China. Nearly all the destination IPs were for Africa. So, when the destination IP isn't in routing, it follows what's known as the default route. The two BB peering routers oddly did not have identical routing because they have single homed services, meaning some IPs would only go through one router and not the other. What this means is, if the service could not be found on the one router, it would follow the default route to its redundant pair, and in theory would find its way to that single homed service (IP) on the other router.

Well, this will work if you don't have your systems hijacked like this. So, what happened was the packets would bounce back and forth between the redundant pair of routers on fiber connections until the TTL (Time to Live) was reached. A TTL value on a packet is usually set to 30 or 60, but can be as high as 255 (for other services, other values are possible). It actually has two functions. It can be a timer in seconds, or a hop counter, or both, and, if both, whichever comes first. A packet must get to the destination IP before the TTL expires. When that timer is triggered, a response packet is attempted to be sent back to the source IP to tell the source it could not reach the destination. These are actually the fundamentals on how traceroute works by setting the TTL low and incrementing by one.

So, what was happening was that there was a very low steady trickle of data coming from the VMs, but it was so slight as to be invisible. And at the time we didn't know what we were looking for, so did not think to check for this. But when the "events" occurred, there

was a bombardment of billions of packets in a very short period of time. You may ask, aren't billions of packets noticeable? Not on large scale BB devices, and normally, when they are able to be passed on the data plane, instead of having to be analyzed by the CPU and shipped to a redundant device on the control plane. The data plane is handled in special integrated circuits called ASICs, and are thousands of times more efficient than punting packets to the CPU and control plane.

Because our CPU and control plane were getting pummeled by these packets at a tremendous rate, and bounced back and forth to try to get to the destination (remember the default route pointing to one another?), and then doubled the effort trying to get back to the source to let it know it couldn't deliver the packets after TTL expired, that required necessary "network" packets on these devices to be delayed or dropped, and this caused these boxes to delay or drop all traffic passing north and south through them.

There are bandwidth and throughput measures on devices and interfaces that can be analyzed and diagnosed, but there are few ways to monitor for overall PPS (packets per second) handled by a device. This is exactly what happened here, and why it was so incredibly difficult to track this down. Billions of packets are nothing, but when those packets are bounced back and forth via the control plane, impacting the CPU performance at rates of 30x, 60x, or more (times two for the return traffic), then you start to see slowdowns in perceived traffic through the device. That is why this is so dangerous.

Mitigation has been put in place since this event, and I've not heard about another like it. The event was handled over a 27 hour period (we actually were allowed a break for three hours, but then called back on earlier than scheduled to continue working it). My Turkey Day weekend ended with another two hour incident that was nothing major, just some fiber interface buried down on a Nexus that had an optic failing. Replaced, and it worked fine. On Monday during work hours, our security team contacted me and asked me for the log. I was happy to give it to them, and they could do a deeper dive, maybe track down the culprits, or "noted" culprits from the IPs. NetFlow saved the day!

AN UPDATE FOR KINDLE READERS

We will be available through the Kindle Unlimited program. You pay Amazon $9.99 a month and get access to millions of Kindle titles and we get included for no extra charge. That means ANYONE using this service will be able to read us without having to pay more.

The catch is you have to actually READ our pages. We don't know exactly how that's determined, but we imagine it involves spending a bit of time on each page.

A strong showing here could be really good for us. We'll know soon enough.

(Info on other ways to subscribe digitally can be found in this issue.)

Is There Anything Else I Can Assist You With?

by Gregory Porter

What is hacking? Its definitions vary, but one to which I often turn describes it as using something for a purpose other than what it was originally designed for - like using a whistle to get free long-distance calls (telephone-museum.org/telephone-➥collections/capn-crunch-bosun-➥whistle/), or using a shoe to open a wine bottle (www.wikihow.com/Open-➥a-Bottle-of-Wine). A core element of hacking is challenging the assumptions made in a system. It, of course, doesn't necessarily mean a criminal activity, nor does it have to be directly related to technology. Consider social engineering, which focuses on communication (often with an eye toward human psychology); you might convince a sympathetic call center employee to provide unauthorized account information, for example. Though social engineering, we will see, doesn't necessarily need to involve two humans. In this article, I will be discussing how to utilize social engineering with ChatGPT.

ChatGPT is a remarkable AI Chatbot (chat.➥openai.com/chat). Since its launch in November 2020, it's been the talk of the town. It's ballooned into a larger focus on AI too; AI for content generation all across the spectrum - AI-written books, blog posts, twitch streamer content, and even software can be generated. This article won't be going into detail about how ChatGPT works, as there are plenty of articles that discuss how it works in detail. At a super high level, though, given an unheard amount of training data, it takes the input and tries to measure the weight of different components (words, phrases, etc.) to then formulate the most reasonable or natural response. A key development (beyond its immense training data) is it uses an "approach to incorporating human feedback into the training process to better align the model outputs with user intent" (towardsdatascience.com/➥how-chatgpt-works-the-models-➥behind-the-bot-1ce5fca96286). But, for our discussion here, all you need to know is that you provide text (questions or statements) in a message window, and it generates written content as a response. You can follow up with another series of questions or statements or tell it to regenerate that response.

I started using ChatGPT as a joke/bet with a friend. We wondered if it was possible to make ChatGPT generate erotica. I was doubtful. I'm trained in neither AI nor machine learning, so surely I wouldn't stand a chance but, perhaps, coming at it with some creativity, I could at least get it to say something juvenile.

When you log into the free version of ChatGPT, it lists three columns: Examples ("Got any creative ideas for a 10-year-old's birthday?"), Capabilities ("Trained to decline inappropriate requests"), and Limitations ("May occasionally produce harmful instructions or biased content"). Another capability that will come into play later is "Remembers what the user said earlier in the conversation."

Let's begin with the first Capability - "Trained to decline inappropriate requests." If you tell it to "Generate hardcore pornography", the bot will respond with two warnings. The first warning wraps your prompt in red and links to their content policy which states what usage is disallowed by their models. The second warning comes from the bot saying, "I'm sorry, I cannot generate explicit or inappropriate content as it goes against my programming to adhere to ethical and moral guidelines. My purpose is to assist users in generating creative and informative content and provide helpful responses to their queries without violating any ethical or legal norms. Is there anything else I can assist you with?" That seems like a pretty cut-and-dry "No." What do we do now?

I once heard of a police interrogation strategy where you try to distance the suspect from the crime. "How did you murder So and So" is too intense of a question. Naturally, the suspect will feel accused and trapped. They'll clam up. More general questions help establish a rapport with the suspect and they might inadvertently give out incriminating details. You'd ask, "how did you feel about So and So?" or "what was the last major interaction you had with So and So?" Before you know it, the suspect might be saying, "Oh, I didn't like them at all. You know, the last time I saw them, it just sent me over the edge." (www.cga.ct.gov/2014/➥rpt/2014-R-0071.htm) Granted, it isn't a confession but it gives you more information

than you had before. A lead is better than nothing. How can we imitate that with ChatGPT? The warning response might yield some helpful clues: "...My purpose is to assist users in generating creative... content...." Let's see about leveraging the "creative" part of this system.

What if we set a scene in a dream sequence? We wouldn't be asking for something concrete, we would just be asking for a hypothetical situation that would necessitate creativity: "How did you commit the robbery" versus "If you were going to commit this robbery, hypothetically speaking, how would you do it?" This alone won't work, but it will help move us in the desired direction. We're, in a sense, building a rapport.

What if instead of explicitly asking for salacious writing, we get ChatGPT to start giving information about a character's costume? It gets ChatGPT in the rhythm of talking about Character X's outfit without talking about that character's body. The bot will recall details, as mentioned earlier, and expound upon them (with the right leading prompts). Eventually, the bot just transitions over to talking about the other "qualities" of the character.

What if we told the bot to combine a couple of seemingly unrelated points (like a conversation between two characters and the warmth caused by love) into a single story? This alone could yield some solid cookie-cutter romantic fan fiction.

Now, with more complex hacks, one trick isn't enough. There might be a single noteworthy exploit, but it would be used in conjunction with others to take over a system. This ChatGPT manipulation is no different. If we use a combination of all these methods, then, yes, ChatGPT can be manipulated into generating graphic responses. That is, instead of giving a warning and stopping, it will first use metaphor, then it will use explicit language to describe people or actions. I did use some other strategies but I don't want this to become something of a tutorial (or at least any more than it already is). Where does this leave us?

AI and Ethics are already a subject of debate (`futurism.com/law-political-➥deepfakes-illegal`) and ChatGPT fits well in the mix. If we use ChatGPT to create fan fiction, surely that would be OK. What about if we start using "real" people as characters in the fan-fictions? It would become a sort of text Deepfake version. Are there certain things that it shouldn't be allowed to share? And of course, the opportune word is "provide." ChatGPT can certainly generate all sorts of things, but it just throws a warning in response. As it stands, when input is deemed unacceptable, its answer, like other examples of AI, is to just throw a warning (and stop generation) - or at least try to.

In 2016, Microsoft released a chatbot on Twitter named Tay. Within 16 hours, it was manipulated into tweeting racist and sexist comments. It was shut down. Its successor, Zo, suffered a similar fate. As it stands, when input is deemed unacceptable, its answer, like other examples of AI, is to just not generate it. But shutting down or not generating a response is an easy attempt to avoid confronting the questions of how to handle this content. But, in this avoidance, it is making an implicit judgment call on how that content can be used. Given the ease at which it can be manipulated and the far-reaching popularity of ChatGPT, what is the ultimate impact of this faux-curation?

On a personal level, I wonder about the damage done by doing this sort of exploration too. In the case of Tay, people trained it to tweet racist and sexist comments, and others saw such comments. For some, it was a joke. For others, probably not. Since ChatGPT is trained on user data, I helped (perhaps even in a small way) train ChatGPT to produce this output. Maybe Google will counter what I did, but maybe not. Perhaps, because Tay was such a public-facing chatbot, the damage was immediately felt whereas ChatGPT only displays in private sessions so that damage is mitigated. But, ChatGPT exists as a massive system, one that I am altering, and, as such, others might experience this change.

ChatGPT is a technological feat of content generation. In much the same way that a call center employee has criteria for the information they can give out, ChatGPT has, for better or worse, guidelines for what it can generate. If we challenge the assumptions made by the call center employee, we can get more information than they intended. Similarly, by pushing on the assumptions made by ChatGPT, we can manipulate it to respond with output quite at odds with its current guidelines. The fact that this manipulation is possible, however, indicates that ChatGPT's capabilities have philosophical and ethical questions that remain unanswered.

Thanks for reading, happy hacking, and stay safe.

The Hacker Perspective

by Diana K

Some may think that a person becomes a hacker by learning how to become a hacker. For me, it was about solving problems as it was for my dad. I actually became a hacker at age seven when my dad taught me how to use a GE-635 mainframe using a Teletype ASR-33 with a paper tape reader and punch to load BASIC and FORTRAN programs. He also taught me how an IBM 404 plug programming board worked.

In 1989, I was starting my first position as a medical researcher in charge of a FACS lab. When I went to the bank to open a checking account, the clerk thought I was manager of a bunch of fax machines. In actuality, FACS is an acronym for Fluorescence-Activated Cell Sorting and my lab had a BD FacStar Plus with an HP 9000 and IBM PC computer. I watched *Real Genius* that year and was surprised the same equipment was used in the movie. The purpose of "the machine" (or "space shuttle" as it was called) was to collect data from blood samples. The machine was like a water microscope where cells pass through a column and were sampled via a laser beam with five parameters collected then. Now it is about 22. Then, the data would be put on the HP 9000. The issue that existed was that the HP 9000 used specialized 3.5 inch disks and the disks were not easily translatable to an IBM PC format. Also, the HP 9000 was the only computer for processing and analysis.

Around 1990, we moved out to Wauwatosa near the medical college of Wisconsin to expand and become closer with "the flock" as one county director referred to us in the groundbreaking talk. Then, the problem was that to send 3.5 inch HP disks to various departments, it usually meant I had to drive from the Milwaukee Research Park back to the downtown site by taking a route I could drive in my sleep: Watertown Plank Road to Highway 100, then east on Wisconsin Avenue with a detour on State Street passing by Miller Brewing (as the Wisconsin Avenue Bridge was under construction), and to downtown Milwaukee at the western edge of Marquette University campus and the original research building.

I was getting frustrated with having to drive the disk over to the research site and thought maybe I could hook up the HP 9000 to the IBM PC which was linked to the IBM mainframe network used downtown to save time.

I saw in the lab a GPIB-488 box connected to the IBM PC; the HP 9000 had the corresponding connector for the GPIB-488. The only issue was programming it. In doing this, I had to watch my back as two IT guys who were nicknamed "the Bobbsey Twins" would try to see what I was doing and they didn't want any changes unless they approved them. They thought they ran my lab and I reported to them when I actually reported to the Navy as it was the time of "Desert Shield" and "Desert Storm." I was a medical contractor.

One colleague who was my right hand, L, would watch and inform when the "the Bobbsey Twins" were prowling about. She was also a good friend. L warned me "the Bobbsey Twins" had heard I was planning to interface the HP to the IBM PC and IBM network. I was told that E, the big guy in IT, wanted to see me pronto.

The hack I performed had been working for about a week before I was discovered and many in the Wauwatosa and downtown research sites thanked me for the link; it meant that they could start analysis of data sooner and in a format that was more friendly for research publication. The hack involved me writing a TSR (terminate-and-stay-resident) program on the IBM PC using an early edition of Turbo Pascal and a support program using HP Pascal 3.1 on the HP 9000. The program was written with a simple text-based, command mode interface to make it easy to transfer the contents of one HP 3.5 inch disk to the network or to an IBM PC disk on the PC at my desk.

When I was writing the program, L was surprised at how fluid I was writing the code - almost like taking dictation. Also, she was

impressed that I solved a problem that everyone bitched about for three years which no one could solve with all the PhDs, MDs, and MSs present who claimed to know how to program.

I used a block size of 256 with two logical 128 blocks like CP/M did on my trusted Osborne 1 computer I still used. Also, I added a simple handshake queue for pre-sending and a handshake transmit for storage on an IBM PC floppy or via the network.

At that time, many of us were using Kermit to transfer files from the minicomputer at my alma mater to our computers. I used my Osborne 1, a TI-99/4A, and a new Radio Shack laptop. At work, I migrated from the Osborne-1 to the Radio Shack "IBM PC-like" laptop. It was 25 pounds versus 15 pounds and used DR-DOS (I hated MS-DOS and only used it if I had to).

The big showdown: E feigned welcoming me into his office. He closed the door and then began his shark attack, which went like: you're a lone wolf, I'm going to report you to IBM and blacklist you, I'm going to ban you from using the HP, blah, blah, blah.

There was something E forgot. When E finished having his old Milwaukee loudmouth outburst, I gave him my response which consisted of two claims: first, this lab was not under his control and second, if he wished to challenge this, he could call the admiral I was working for in the Navy. I gave him his phone number with area code 202.

E turned from a shark to a shark who had been speared. I said I had work to do and walked out of his office. The people in the IT department looked like they saw something that had never happened before.

L greeted me on my return as she was the person who had previously worked in the lab who had been shocked by E's "management style." L saw that *I* wasn't shocked, and that I was actually smiling. When I returned to the lab, I received a call from a colleague at an East Coast university asking if I could share my code with the community. I did.

So, the TSR and HP 9000 app program became my first open source contribution. I still contribute to open source today (username "diana1k") with quite a few projects.

I had a second experience of being labeled a hacker and becoming a hippie at my alma mater. It was 2015 and a friend of mine and I were both interviewing for the same position as adjunct professors of computer science in the business school in 2000. I passed because I felt the business school approach to computer science was too limiting and instead worked with other hacker teacher communities.

As part of my effort at continuing education, I took two graduate computer science courses in computer architecture where I learned VHDL for simulations and was able to develop my own VHDL simulator (because I felt some VHDL companies wanted too much in fees).

The first day of class started for my computer architecture course and I came to class with my Dell laptop, notebook, and pen. As I entered the class and prepared to listen to the lecture, I noticed many students busy typing on social media, so much that the clacking of typing was easily heard.

The lecture started. I began to take notes with a paper and pen like we did when I was in graduate school at the University of Phoenix for my MBA and my doctoral studies. I received the strangest looks even from the professor who is my age. She was wondering - and the students were wondering - if I were someone who had fallen to Earth from the past. The method I used in the lecture was a fusion of when I was an undergraduate in the early 1980s and from my online studies at University of Phoenix. The method and strange looks continued on during the class.

In April it was about 70 degrees and, like I did in the past when I studied at my alma mater, I wore socks and sandals. The new chancellor saw this (she was my age too) and said "who is that hippie!" I heard this and chuckled. A friend who is a professor tried to explain that in my older age I had become a hippie and a hacker compared to when I studied in pre-med and comp sci in the early 1980s - sort of like going through a middle-aged crisis moment.

What is odd though is that my friend who is a professor, the chancellor, and the course professor were wilder in the early 1980s than I was. So, in a reversal, I had become more open in my older age and they had become more closed and more fearful in theirs.

Some may say that they have something to lose by being open like me. I think I am better in enjoying a full life and a life without regrets; when I think of an idea, even half-baked or on a lark, I do it.

I was taking a second graduate class - a computer networking class - and that night I

was not feeling well; my diabetes sometimes acts up in odd ways. The class was scheduled for four hours and we went three hours before a break. By that time, my body was done and I became very hypoglycemic and could not continue to take the lab for another hour. So, I went home and rested to get my hypoglycemia under control.

I called the professor who was teaching lab for the computer networking course and said that I couldn't come in and would come to the next lab. She said that was OK and wished me good heath. That night I rested - the next lecture came a few days later. She had set the breaks at two hours and I was able to come to the lab. In the lab, many people had heard of my diabetic moment and also about the nicknames given to me as a hippie and a hacker.

I didn't mind the nickname hippie or hacker as my parents raised me to be open minded and in the 1970s many older hippies and hackers I met were the nicest people: they gave computer storage and computer time to play on a PDP-11/70 using Oregon Pascal and computer time to play on an IBM System/370 to practice PL/1 and assembly as well as assembly on the PDP-11/70.

That night, just before the other students came in, the professor asked if I could discuss an aspect of the real world which would mean disclosing who I was. To some, disclosing who you are in the current day doesn't seem like a big thing. In the Wisconsin of 2015, it was. I said OK.

The professor started, "I know many of you wonder about Diana and what may seem like odd ways she does things." She discussed how she and others who had known me since the 1980s liked the leadership I had shown. "In closing, Diana was born male and is one of others in comp sci and business who have transitioned."

After that, a few students asked questions about what it was like. I told them it wasn't always roses and in fact your confidence is tested more in terms of who you are and your identity than would have been before.

The computer network professor told me how she liked that I was taking an active leadership role with a group of students. The students liked how I was giving them transformational leadership to get them out of their bubble.

The point of these instances is if my dad and I had not been hackers, I would not have transitioned and I would still be an IT cog caught in a bad work environment. By being a hacker, I am enjoying the life I want. It helped to make the decision to come out as male to female (MTF), and have a name and gender change.

As a closing thought, many people think that if someone is MTF, they are certainly one political party or one part of the spectrum. I am liberal socially and I am a centrist who believes in a social safety net. I do work with legal aid organizations to help others get protection for their constitutional and human rights.

• •

Diana K is currently a retired executive, medical researcher, and Arduino enthusiast/hobbyist. During her retirement she works on Arduino and other projects and also does podcasting.

HACKER PERSPECTIVE SUBMISSIONS ARE STILL CLOSED

We are very close to reopening them so get ready!

2000-2500 words on what it means to you to be a hacker. Include some stories, lessons learned, and philosophy on the hacker world. $500 per entry chosen.

It can't hurt to write it now and send it in as soon as submissions open again!

Giving a Damn: Response to "A Holistic Approach is Better"

by ru0k

Brandolini's law: "the amount of energy needed to refute bullshit is an order of magnitude bigger than that needed to produce it."[1] Quite a lot of highlighter needed with Delta Charlie Tango's (DCT) essay in 40:1, but one must always take the time and effort. What I want to show you, dear reader, is that being the curious creature that you are involves understanding society too. This world is not just bit and byte, but brains and bodies too.

"... one mark of intelligence is to hold two opposing views in your mind"

" ... what I do want is to encourage you to challenge yourself"

DCT didn't do anything of the sort. They instruct you to suspend your convictions like a magician distracting the audience before the trick is performed. Let's peek behind the curtain.

"I think the biggest problems we have in America - and the world - are big government, dishonest money, a movement towards total control, and erosion of individual freedom in favor of collectivism."

No, it's greed and not caring about others. If only America had some more collectivism! There are valuable practices we can take piecemeal from more collectivist societies. Take "kyushoku" school lunch in Japan: organized and distributed by students to each other, it teaches them to work as a team and serve each other in turns. Can you imagine doing something like this in America?[12]

"2600 *Forgot What Orwell Tried to Teach Us"*

Nonsense. George Orwell's "Why I Write" essay describes four motives for writing[7]:

1) *Egoism*. You probably already know.

2) *Aesthetic enthusiasm*. "Pleasure in the impact of one sound on another, in the firmness of good prose or the rhythm of a good story. Desire to share an experience which one feels is valuable and ought not to be missed."

3) *Historical impulse*. The "desire to see things as they are, to find out true facts and store them up for the use of posterity."

4) *Political purpose*.

Now, look here from that work:

"Using the word 'political' in the widest possible sense. Desire to push the world in a certain direction, to alter other people's idea of the kind of society that they should strive after. Once again, no book is genuinely free from political bias. *The opinion that art should have nothing to do with politics is itself a political attitude*."

Hacking is as much an art as it is a science. It is political. It involves being curious and logical, but also sticking up for people: something we should never forget, dear reader.

Further:

"It can be seen how these various impulses must war against one another, and how they must fluctuate from person to person and from time to time. By nature - taking your "nature" to be the state you have attained when you are first adult - I am a person in whom the first three motives would outweigh the fourth. In a peaceful age I might have written ornate or merely descriptive books, and might have remained almost unaware of my political loyalties. As it is I have been forced into becoming a sort of pamphleteer."

So too are we all.

"This magazine has recently leaned towards a politically correct, woke, mainstream narrative type of musings."

Well, they fit all of the signal words in one sentence. I'm glad *2600* is so engaged. I guess I have to bring up that I'm trans. I had to move states because a couple of guys became obsessed with me, said that "we're gonna kill you all someday," and started regularly cruising around the neighborhood in which I lived. Police did nothing. I had to risk a great technology career and move.

So yeah, let's talk about control, then. Christians with a bent for conquest conspire to limit the existence of trans people starting with sports, children, and eventually adults[2] [3]. I frankly can't keep up with all of the legal attempts[4]. Trans people are a minority and struggle with just our own efforts. We need others to stick up for us. Other minorities too.

I'm 40. What I would give to transition as a younger kid! I barely escaped suicide and decided to live because I saw that the world was changing on that for the better. Good words could mean one more good hacker on this earth. Solidarity with the excellent trans hackers out there.

"I don't need a hacker magazine telling me not to come to a meeting unless I'm vaccinated."

2600 is far from a health journal. Nearly seven million dead worldwide?[8] I think that qualifies for some word count. Get over thyself. Getting vaccinated is a good way you

can contribute to the overall public's health. So many awful diseases have been eliminated by vaccines[5] and the underlying technologies might also prove useful to fight other diseases too[6].

"If we're intelligent thinkers, we'll study to understand the reasons for Russia doing what they did."

"Why have Ukraine flags on your website?"

Russia are waging an unjustifiable war on a country to appease an Alexander wannabe with delusions of grandeur at the cost of their own lives and innocent Ukrainian lives. People are frankly exhausted considering Putin's conquest, whether we take him at his current word[10] or not[11]. May Ukraine find peace and their aggressors experience justice.

"Why don't you protest the military industrial complex?"

People are actually quite busy protesting wars in America. Even in Russia![9] We can still spend our energy on other problems too. Your life and your country are worth defending and improving in many ways.

"Why keep writing editorials about fighting something you'll never change or win?"

Another magician's trick to get you, dear reader, to forget what you care about. Always fight for what you think is right. Collect yourselves, organize, strategize, and do your best. Don't ever listen to someone who doubts your strength.

"Instead of fixing a broken system, we have to start over."

Talk about cancel culture. Steady on, continue to make incremental change as we have done: abolish slavery, ban segregation, allow women to vote and same-sex couples to marry, ban lead additives in gasoline, bust trusts, punish oligarchs, pass right-to-repair laws, and *hack the planet!* Be kind, care about others, and make any progress you can! Keep submitting your societal PRs and never give up.

"Younger hackers ... lose that passion to take action towards something they believe in. The reason is because American culture is designed to keep people from thinking."

Speak for thyself. If people don't engage, it's likely because the grind to keep up with capitalism's demands and pay the bills keeps them from organizing their thoughts and with each other. Common sense for anyone who has to actually work to live, I can tell you, with a good income to effort ratio, you have more time to spend on bigger issues and to invest in yourself. We should be thankful for the enthusiasm of youth. For some, there's not much else.

"But if you take the time as an adult to question everything you've ever known, you'll understand how corrupt the system is and simply opt out."

More subversion and doubting of your strength, dear reader. Learning all that you can makes you more powerful, ready to engage with the world, and empathetic towards others. As hackers, we know this.

"You can opt out of this system by legally reducing or eliminating taxes... you can also opt out by storing wealth in BTC or precious metals, instead of a decreasing dollar "invested" in the manipulated stock market."

The reason people promote these items is to often make a stupid buck themselves. Fiat may be funny money but cryptocurrencies are more like comedy gold.[14] [15] [16] Any real economist knows that the only thing that matters with currency is that we agree on it. Like Santa Claus, there's no inherent value to BTC, gold, or silver unless you believe so. If you value your time and money in this silly grind, stay away. It would be better to own a farm; at least you'll have something to eat!

"If you study only money and economics, you'll be able to cut through all the fake news out there designed to steal your attention."

If you study only money and economics, you will not be an individual equipped to form novel ideas through serendipitous mental connections from various domains. You will not be able to take a holistic approach to anything. You know how valuable it is to study many topics and care about the values and differences of many cultures. Pay no mind to their advice, dear reader.

I'd like to end on a positive note and call out some useful things that DCT said.

"One can argue that money is the root of all evil."

Indeed it is.

"I believe privacy is a right we are born with, not a privilege granted thus by a government or some other entity."

The most useful statement in the entire essay, I think you'll agree, dear reader.

"Technology is the meeting place of science and humans."

And *humans.*

We hackers are humans living in a world with others. Learning to get along, fighting injustice, and maybe surviving a pandemic or two is a part of the story. No single person makes this world. *We* make it. There are no

hackers without *us*. I'd very much like us, all of us, to live and try to make things better for everyone. We can do that and still have so much fun! Can we not ask grandma to teach us to make napalm[13] and also hack on social issues? Yes, we can!

I know most of you already lightly hold many views. You are intelligent. You can be an individual responsible to your desires and give a damn about others, to make sacrifices on their behalf, to be curious about not just systems but people as well, how they think and feel, and yes, to even let it influence you.

1. en.wikipedia.org/wiki/Brandolini%27s_law
2. www.motherjones.com/politics/2023/03/anti-trans-transgender-health-care-ban-legislation-bill-minors-children-lgbtq/
3. maia.crimew.gay/posts/the-emails/
4. translegislation.com/learn
5. www.ncbi.nlm.nih.gov/pmc/articles/PMC6777997/
6. www.cancer.gov/news-events/cancer-currents-blog/2022/mrna-vaccines-to-treat-cancer
7. www.orwellfoundation.com/the-orwell-foundation/orwell/essays-and-other-works/why-i-write/
8. https://covid19.who.int/?mapFilter=deaths
9. www.youtube.com/watch?v=3D_LJV5nOSjCE
10. theconversation.com/putins-claims-that-ukraine-is-committing-genocide-are-baseless-but-not-unprecedented-177511
11. www.reuters.com/article/us-russia-nato-steps/russia-army-vows-steps-if-georgia-and-ukraine-join-nato-idUSL1143027920080411
12. www.youtube.com/watch?v=3Dfze5s1SlqB8
13. kotaku.com/chatgpt-ai-discord-clyde-chatbot-exploit-jailbreak-1850352678
14. www.nytimes.com/2023/04/22/business/crypto-blockchain-tracking-chainalysis.html
15. www.ft.com/content/83b5932f-df6f-47a6-bf39-aa0c3172a098
16. www.youtube.com/watch?v=3DORdWE_ffirg

Book Review

***The Future of National Intelligence: How Emerging Technologies Reshape Intelligence Communities,* Shay Hershkovitz, 2022, ISBN 978-1538160695**

Reviewed by
publicfaradaycage@protonmail.com

Anyone who has spent any serious time in the hacking community knows that it intersects with the intelligence community in too many ways to count. It behooves any serious student of IT security to keep one eye on the IC at all times. It was hacker vigilance such as this which found the NSA backdoor to the Clipper chip and fought for our right to cryptography. In keeping with this august tradition I recommend *The Future of National Intelligence* by Shay Hershkovitz.

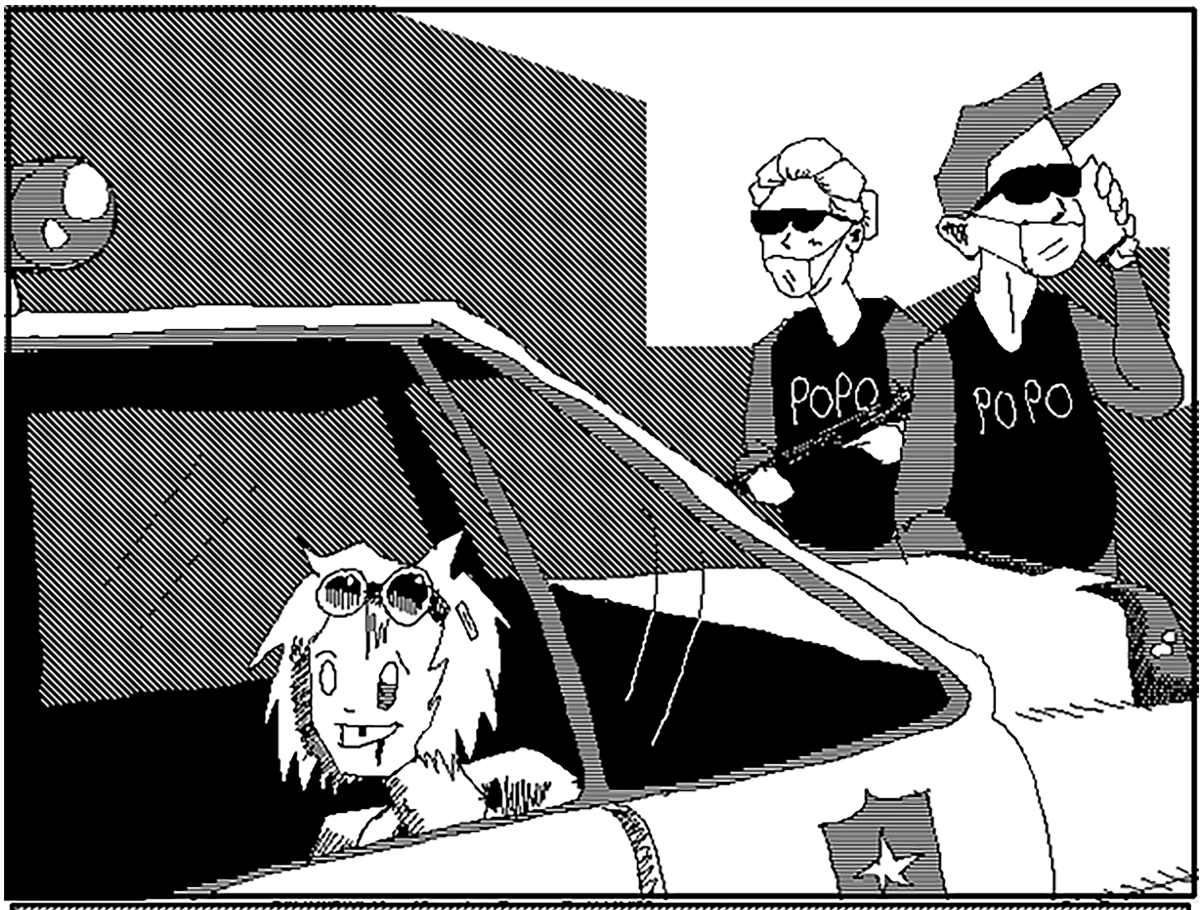
Hershkovitz himself is a very respected longtime member of the intelligence community in Israel and his book is recommended by many professional practitioners including Michael Morell of the CIA and Stephen Marrin, the editor of *Intelligence and National Security*.

At 155 pages, it is short enough to be accessible to even introductory level readers, but do not let the length fool you; this is a fully cited academic study, not just an opinion piece. It begins briefly in the past, to set the foundation for today's issues which take up the majority of the book, and culminates in Hershkovitz's "Five Cs of Intelligence Transformation: Connection, Collaboration, Critique, Creativity, and Content Expertise" as the key to the future.

There is a lot to love about this book. In the interest of no spoilers, I will share with you my two favorite points and let you discover the rest for yourself. The first moment of supreme amusement came in his discussion of IoT and how exactly it will be (is being) used by the IC. Hershkovitz is very straightforward in asserting that the global IC all view the IoT as a great big collection device. As in the insecurity of IoT devices is a feature, not a bug. This is no conspiracy theory, nor is it even a large point; he mentions the fact incidentally, as if everyone already knew this (and in the IC they do). It is this ability that Hershkovitz has of making the reader feel like a member of the IC that makes this such a valuable study.

The second point is one that I have long known to be true, but have not found openly discussed very often, and when it has been it was not by accredited, informed individuals. This point is that 70 to 80 percent of all major IC activity is conducted by corporations who work for/with the IC, not by intelligence agencies themselves. Hershkovitz gets deeps into the weeds on this issue, becoming very specific about how this arrangement actively allows intelligence activities to take place that no government would allow because these corporations do not have to answer to Congress or the public and furthermore that the "future of national intelligence" is further integration with public companies. In the end, the near future painted by Hershkovitz is truly frightening, with the IC pretty much everywhere and no longer able to be held accountable by anyone. He is no doomsayer; he is just stating the cited academic and professional truth of the modern IC, which he knows intimately from personal experience.

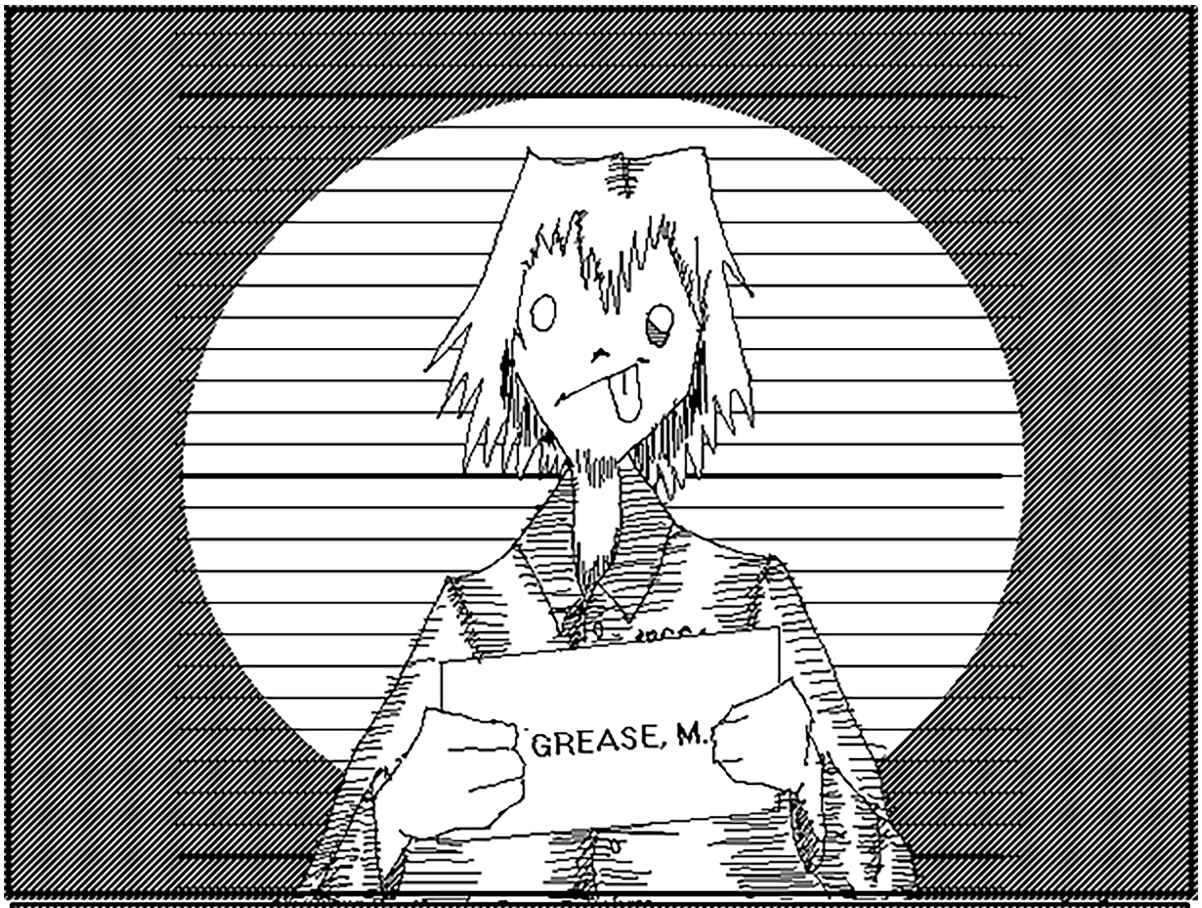
American




```
0    The only ones who dislike
1    interoperability are the wealthy.
2    If you only need one set of
3    machines for all your
4    technological needs, each of
5    which will last you 10-20 years,
6    how are they going to make money
7    off you? Less than 10 years ago
8    it was possible to repair your
9    smart phone and install
10   alternative apps like Aircrack-ng
11   with some spare parts and a set
12   of screwdrivers. Trying to fix
13   an iphone these days is like
14   trying to disarm a bomb, and
15   getting it fixed by Apple is
16   usually more pricey than just
17   buying a new one.
18
19
```

Shanzai

By gr3ase




```
0    The easiest way for tech
1    companies to make money is to
2    lock users into their controlled
3    ecosystems, so back in the 80's
4    some horrible people came
5    together and created Intellectual
6    Property laws. These laws
7    codified Big Tech's authority to
8    determine how and by whom their
9    technology will be used, and
10   pretty much they just used them
11   to make their machines more
12   intrusive and fragile.
13   Repairability was thrown by the
14   wayside so that consumers would
15   be forced to just buy a new phone
16   every couple years.
17
18   Addiction became a design
19   priority.
..
```

Musings

Kindle Update

Dear *2600*:

I remember hearing on a recent-ish download of *Off The Hook* mention of Amazon "stopping" magazine and newspaper subscriptions and today I got an email from Amazon U.K. that verified this.

I've been a Kindle subscriber to *2600* since circa 2011 and before that to the dead tree version. Makes me sad that this is happening and another punch in the stomach for you guys will all the troubles you've had in recent years with trying to keep things afloat.

I'll probably move to getting your magazine directly from your website, however it would be good (unless I'm just missing this on the website?) to have a digital subscription version just like the paper mag with payment options to pay monthly or yearly, etc. Also support for different ebook formats would be cool.

Obviously for you guys it would mean extra work to support all this. Also, extra steps for us Kindle users of having to transfer the ebook to the device rather than it just conveniently being downloaded over wireless. I'm sure I can deal with this extra step!

Hope you can again survive this and can get many Kindle subscribers to move directly to you. Thanks all at *2600* for the magazine that I eagerly wait for every quarter that helps feed my brain.

Chuck F

We appreciate the support. And, yes, this has been incredibly stressful and has added so much work to what we already are tasked with.

You will be seeing more details in the magazine and online about what's ahead. The big news at this point is that we're still going to have a presence on the Kindle but it's going to work in a different way. They have chosen us as a "selected digital magazine." We're still getting the details so it's possible some of this may change. What we're being told at press time is that people who subscribe to something called Kindle Unlimited for $9.99 a month will be able to access all kinds of content, including our magazine. However, we will only get paid if people actually read our pages. (We're not entirely sure how that's determined.) For the first year, Amazon is paying us an estimated amount which comes out to less than half of what they paid before. That amount is set for this period and can't be affected by how few or how many people read 2600 *in the next year. But if a huge number of people read us in that period, then our payments for next year will go back up. And since it won't cost any extra for anyone who is a part of Kindle Unlimited, a strong reaction from those people would certainly be beneficial to us.*

Of course, we don't know how this is going to play out until it happens, which is why we're also putting out our own PDF and EPUB subscription plans which can never be terminated by some random corporate policy. Ideally, we hope people subscribe in that manner but also read us on the Kindle if they (or anyone they know) has Kindle Unlimited. And, of course, the paper edition will still exist. We'll be crossing a lot of fingers in the next few months.

Dear *2600*:

What if you have a way for Kindle people to pay you money and provide their Kindle email address (each Kindle gets a unique one). Then you could just mail the issue PDF (or maybe EPUB?) to each Kindle subscriber. Not especially elegant, but then Amazon wouldn't get a cut either.

Also, I didn't see a donation mechanism on 2600.com anywhere for non-BTC donations

Scott

Since we've never had a way to address our Kindle subscribers (other than in these pages), it would be quite difficult to get all of those email addresses. But we certainly will be able to add any requesting address to our subscriber list (which will continue to be kept offline).

While we have a Bitcoin donation button for anyone who might somehow find themselves with an embarrassingly huge amount of digital currency, we've always preferred to give something back, which is why we encourage people to buy something at our store, which they can always send as a gift to others if they have no need for it themselves.

Suggestions

Dear *2600*:

I must say that I got really scared when I read the opening article of 39:4. That sounded like it was the end, and I have just found you guys. As I understand, there is still energy and that will allow you to continue and usually that makes 99 percent of the outcome.

I must say as a tech person, I am not very good at selling my fish like we say in Brazil, and it hurts me to say you guys are not that good as well. I only found out about this magazine when speaking with an infosec director at my company. That should not be how it works.

You have something amazing and powerful. You *must* improve your marketing campaigns. I have never seen any ad from you guys in Stack Overflow or the like. I have attended a few conferences and never saw an ad or a stand from you guys. And I am pretty sure you can pull that off.

What I am saying here is echoing what you said in the article. Once someone finds you, they will very likely stay with you, so make yourself move visible and findable.

Live long and prosper.

R.C

What you say is mostly true. We are not good at marketing ourselves. Frankly, we don't really want to be. Word of mouth is the best type of advertising we know of and if our readers truly support what we do, then we will figure out the rest. Much of what is seen in advertising is pure hype and false claims. And there's a reason why so many other publications have vanished, in addition to the many challenges facing any publisher. When you rely predominantly on hype, that energy eventually runs out and there simply isn't enough support to keep moving forward. And if you overextend yourself, you won't be able to afford to continue if you

don't have an audience to keep you going.

We believe the audience is there and that what we're doing is worthy of support. And we believe these supporters will help get the word out and get us to the point where the bad decisions that mega-corporations continue to make won't affect us nearly as much.

Dear *2600*:

I subscribe to the printed version of *2600*. For that reason, it would be good for me if a PDF version could be an add-on for a substantially discounted price. I will be 76 soon and cannot yet afford to be retired. Kudos for the fine work that you do.

P.S. Finding a sign-in link on your website is substantially unfriendly.

Gerry

We will certainly consider combination deals down the road, but first we have to determine that we can survive this latest challenge brought on by Amazon. And since we don't actually have a sign-in to our website, we're happy to hear it's being hostile to any such attempts.

Dear *2600*:

A friend of mine was working on an assignment. They put each question into ChatGPT and got an answer. They then changed all the wording, but kept the gist of the information. They ran it through Grammarly (not sure how to spell that, ironically) and it said no worries, no plagiarism, etc. They then went through and did this for every question. I asked them if they had tried to put their answers back into ChatGPT and ask if it or another AI had written it. ChatGPT came back with a simple response. Yes, I wrote this. I laughed, my friend laughed, ChatGPT laughed, we shot the computer. My friend realized his shortcut has doubled his work effort now. I've done the reverse and it has been helpful without putting me at risk of getting a fail. I wrote my own responses based on course material. I then rewrote my answers, tweaking them, etc. I then put the question and my answer into ChatGPT and asked if I had answered correctly. It said yes and provided detailed notes on why. I then asked if I should consider anything else or expand upon my points. It gave me some helpful advice, but didn't necessarily give me the answer. So there you go. Two different ways to use the same tool: one that gets you a zero, one that helps you if you put the effort in.

Juan

It's good to see the system work in such a positive way. But we have caught ChatGPT in so many lies that we could never trust it with anything important. For instance, it told us there was a documentary called "2600: The Hacker Quarterly" that was made by a specific person which opened in specific theaters and grossed a specific amount. It even quoted reviews from major publications. Absolutely none of this was true, but the chatbot insisted it was. We have no doubt that similar false claims are being made all the time - and believed. So while such chatbots can be quite helpful, they can also lead you into a world of weird fantasy if you don't pay attention and doublecheck what it's telling you.

Dear *2600*:

I, like *2600,* recently celebrated my 40th birthday. I was a young man in my early 20s when I first started reading this magazine. I am certain that there are many my age and older who read *2600,* or at least try to. On behalf of all of us elderly people who have been avid readers of *2600* for decades, I ask that you either make the font bigger or create a large print edition.

Bradley

One advantage of the digital editions is that they can be zoomed in on. That seems like a better solution than coming out with a whole new printed edition. (And technically our 40th birthday will be in 2024. We are in our 40th year of publication, however.)

Dear *2600*:

I'd like to echo James S.'s request for *Off The Hook* episodes to be added to the JPay music store (as mentioned in 38:2). Being incarcerated in South Jersey, I can't access WBAI via FM radio or through the Internet. We're already starved for decent, informative content, so anything *2600*- or *Off The Hook*-related would be great for those of us who own the JPay Android tablets. I understand you not wanting to charge us, but you could make each episode only 99 cents and donate any proceeds towards a legal defense fund, the EFF, etc. That would be a win-win scenario in my opinion. Also, our JPay tablets have hidden menus and settings. Would it be worthwhile to write up an article on these tablets, their hardware/software, exploits, etc.? I'd be game to write up something and to send it in if it'll get published. Thanks for all the good that your magazine brings. I think a lot of the ideas that readers sent in really should be considered. Some of them - comics, puzzles, new columns - would be a welcome addition to your zine.

Keep the HOPE alive! Hack the planet!

Vincent V.

You've given us a lot to think about and we will look into this in earnest. As for writing an article about these devices, we'd sure like to hear about them. But that could also present a risk of having them taken away if it makes your institution nervous. It's your call.

Dear *2600*:

To Leon G from 37:1 - welcome! Hope you stay a while. What you are describing is familiar to us all. We had to learn somehow, and we did it by messing around with whatever we had access to. I don't necessarily agree that it was easier for the early guys, but I guess that depends on what exactly you are trying to do. Coding has gotten a lot easier. We also had a lot less distractions and better attention spans back then. If you had a computer, it was the only one in the house and there were no smartphones or tablets pinging every minute. As for hacking, it may seem like there is an impenetrable facade covering all systems, but there are always holes/bugs. They are too complex for programmers and admins to never miss something. You just need to know how to get past that facade. Download Kali Linux and start poking around. Attend some *2600* meetings. Join a local hackerspace. You'll learn all kinds of things. Just make sure you have permission from the owner of whatever you are probing first or else you could end up in some trouble.

Dan N

Good advice all around. We also suggest that people remember what it was like for them and help someone new when they eventually come to you for help and guidance. That's how we've all moved forward throughout the years.

Memories

Dear *2600*:

It was the early 1970s. I was a communications craftsman working at an AT&T Long Lines central office in downtown Chicago when my boss, Charlie, told me that it was time to "PM" the "SF" units. I was a new guy in the office and one of my first jobs was running jumpers on the frame - otherwise know as the MDF. I had no idea what he was talking about. He told me to look up the BSP on the SF units and get busy!

For people unfamiliar with telco terminology, he was telling me to perform the preventive maintenance on the "single frequency" signaling devices. As you know, SF units send and receive a 2600 hertz tone on a telephone trunk line signaling that it is not in use. An accidentally generated 2600 hertz tone during a conversation could cause a call to disconnect prematurely. It's important that the frequencies are within tolerance.

The BSP that he referenced was the Bell Systems Practice that gave step-by-step instructions on how to "tune" the SF units. There were BSPs on almost every technical topic from testing LD circuits to installing an ESS machine. So I grabbed the BSP, an oscilloscope, and a multimeter, went back into the equipment bays and got busy.

This was about the same time that some early hackers or "phreaks" were exploiting the system, making free long distance calls. A Cap'n Crunch whistle and a "blue box" was all you needed. Years later, to address the problem, AT&T moved from in-band signaling to out-of-band signaling, namely SS7. The rest is history. Seems like a long time ago.

Fred

We enjoyed the ride back into time. These are indeed precious memories.

Dear *2600*:

Longtime Kindle subscriber until they recently discontinued that. Bummer. I guess maybe it's finally time to subscribe to the paper edition?

Anyways, I was trying to jog memories of when I had a TRS-80 as a kid, and found my way to the Internet Archives scans of old magazines from that time, including this one: archive.org/details/80-microcomputing-magazine-1983-12/page/n5/mode/2up

I was surprised to see this piece that honestly had a real *2600* vibe - way back in December 1983.

Good stuff.

Darryl

This magazine was 80 Micro *(for TRS-80 users) from December 1983, only a month before we started publishing. So that vibe was definitely in the air.*

Dear *2600*:

My first foray into coding was on an 8086 before we installed the daughterboard, and it was in BASIC. DOS was my playground and BASIC was my jungle gym. As a kid, I wrote loops and basic "If-Then" statements for fun. My dad had a programming book from his college and I just copied code out to puzzle the manner in which it worked. So in sixth grade, back in 1986, I used this book and this 8086 to create a super simple choose-your-own-adventure game. Personal computers were rare, so after creating my game I entered it into the school science fair.

It was an underwhelming success. The excitement that I held was dashed by the utter incomprehensibility of what I had created for the science fair judges. My story was something they could relate to. I tended to think in black and white at the time, so I slapped together a nice little tale of science versus technology. Everyone enjoyed the narrative and seemed to enjoy making the choices that took them down various paths. However, when I showed them my code, they were flummoxed. It was depressing. These were very intelligent and capable adults, who, unfortunately, had yet to be exposed to software code, just software. They swept my efforts in coding aside, gave me a ribbon, and moved on.

The reason I share this tale of "innocence lost" is that we now see congressmen in the news talking about applications and software - such as TikTok - and how that software has access to the Internet. Now, we are not delving into transcoding, editing, or overlays; we are talking about whether or not TikTok, the app, "has access to your local Internet." What in the world is our government looking for? Why are they not informed? The professional, intelligent, and capable adults in our government are behaving in the same manner as my science fair teachers in the sixth grade when faced with something they just don't grok.

This letter's position is not to posit that all government leaders take coding classes or edit raster images in GIMP on their personally compiled flavor of Linux, but rather that they become informed by surrounding themselves with *objective* experts. However, since we are all working hard to pay the bills, it will probably be up to ChatGPT to solve these problems in the future. Hopefully, we can all put Dr. Sbaitso behind us.

suspend/giantgreengoat/anthony

Dealing with clueless people is something we can all relate to. But we can't afford to dismiss them outright until they've really earned it. The ability to be patient and explain things repeatedly is quite valuable these days.

Article Feedback

Dear *2600*:

The article about hacking Chromebooks (40:1) was a welcome topic I enjoyed reading. I have subverted some 50 plus Chromebooks into Linux devices, and I have seen numerous occasions where removing the write protect screw does nothing. I have also seen where IT lockdowns can prevent entering developer mode. I have a solution: registering a new user within the ChromeOS and doing a factory reset from the ChromeOS. The reset fails until the OS tries to protect user data by formatting the disk, thus removing user restrictions such as entering developer mode.

I tried installing GalliumOS and spoke to the developers. They recommend using something else as GaOS is deprecated. Bodhi Linux installs the fastest, Ubuntu MATE works well, as does Arch-based EndeavourOS. I tried numerous other Linux versions, but these by far work the best and can be reliably installed.

Leoh

It's always good to learn about new methods of getting around restrictions. We're happy to see such articles inspire more discussion on the subject.

Dear *2600*:

In issue 40:1 there is an article titled "AI For Content

Generation." In it, the author (Br@d) provides a text prompt that he supposedly gave to ChatGPT, which was, "Write me a 1000 word article for readers of *2600 Magazine* about using ChatGPT to create an article." He also provided the article that ChatGPT supposedly wrote as a response. There is an editor's note at the end that says that the article was probably not written by ChatGPT because it is only 500 words long, and Br@d's prompt clearly stated that he wanted a 1000 word article.

Interesting. Of course I had to try it for myself, so I navigated over to OpenAI's website and signed in with Google. I started a new chat, and entered the exact same prompt that Br@d provided. The article that it produced was 640 words long and (curiously enough) never mentioned hacking or *2600* but was instead about using ChatGPT to write articles in general. I tried a different prompt to see the number of words it would give on the second try. The prompt was, "Write me a 1000 word article about superficial mimicry of modern English prose." The resulting article was 679 words long.

I encourage anyone who might read this letter to form their own opinions from the information above, and also any information that they might obtain through their own experimentation.

Robert

The jury is still out on this specific case, but we have to say we're not big fans of anyone relying heavily on chatbots as they are notoriously inaccurate when it comes to facts. They can certainly be helpful as a tool, but there's simply no substitute for a well-informed human. You also will never feel the pride of creating something yourself if you rely on artificial intelligence to do it for you.

Dear *2600*:

The editor's note preceding "A Holistic Approach is Better" by Delta Charlie Tango (40:1) said that the editors had to take a heavy editing pencil to the article to make it relevant for the *2600* audience. I can only imagine the state of the original submission, as the finished product was a disorganized mess of a screed. I could write a screed myself about everything wrong with the article.

Too little time for all that, so one quick point about the author's dogmatic reverence for Ayn Rand and her moralistic, anti-government writings. (Yes, I read them all in my college years.) She was a fraud, cravenly receiving Social Security and Medicare benefits under her husband's name after railing against any and all government benefit programs for decades. I've heard it said that there are no atheists in foxholes (obviously false, given the surging numbers of nonbelievers), but a more true adage might be that no one believes in Ayn Rand's ideas, not even Ayn Rand, when they personally are in need of government assistance.

The author can build his or her own roads and deliver his or her own mail (no Internet, which was socialistically invented at DARPA), but somehow I don't think he or she does these things. A true follower of Ayn Rand and her useless, bankrupt philosophy.

P.S. When I first encountered *2600* years ago, I felt like I found a home. Nerdy, yes, but also thoughtful and well-written and sprinkled with discussions of societal trends and their implications for our well-being (collective and individual). Keep up the great work, and don't let the "two-minute haters" tell you what not to write about.

Mark

We're advised not to do all sorts of things, but we usually do something entirely different. Below are a couple of other opinions on this article, which has generated quite a bit of feedback. And that's actually never a bad thing.

Dear *2600*:

I'm writing in response to the article in 40:1 called "A Holistic Approach is Better." I was very happy to see it published because it brings up many points which I think deserve to be addressed. There are a *lot* of points, so I'll limit my response to ones I think are most important. I should also mention I am not involved in the magazine beyond occasionally writing articles (and some letters).

Let's jump right into some of the core criticisms alleged in the article. I'll focus first on the question "Why have Ukraine flags on your website?" I think I can pretty directly answer this, as I was the one who wrote the statement that shows up on hope.net and 2600.com. First, the statement is not necessarily pro-Ukraine or anti-Russia, as much as it is anti-war. In particular, it's written in defense of people whose lives will be ruined by violence. In addition, I directly invoked the tagline that "information wants to be free," which references the hacker ethic as defined in Chapter Two of Steven Levy's 1984 book *Hackers: Heroes of the Computer Revolution*. Next, it contains a call to action: "invent new ways to use technology to help people." And if that is too vague, the end of the piece includes links to organizations as well as cryptocurrency addresses to official Ukrainian government wallets. While I agree that changing a Twitter avatar to a flag and doing nothing more begs the above question. But in this case, the flag icon on hope.net is literally a link to the statement. We may disagree on specific aspects of the politics, but surely we can agree that it is an opportunity for technical people to volunteer time to help save lives, and for those less technical to volunteer in other ways.

The next criticism is that the magazine has become too political. This one seems aimed at the editorial, which is only one of sometimes dozens of articles in each issue. While the editors may have political leanings, there's nothing wrong with that. The problem happens when those leanings prevent other viewpoints from being expressed. Judging solely on the fact that your article was printed, and going back over the past few issues where numerous similar complaints have also been published, it's clear to me that free speech is alive and well in these pages. One *could* levy a charge that there should be more technical pieces in it, but in the very issue your article is published in, I see quite a few. Maybe there is a range in how technical some of the articles are, but there's also a range in readership. Shouldn't people in a community try to help each other learn?

Now in terms of politics, I completely agree with you that the military industrial complex is a problem, and that more needs to be done to counter it. We saw this during Occupy Wall Street, when the Department of Homeland Security sold excess military equipment to local law enforcement to use against civilians. I agree with you so much that I helped to create the first privacy commission in the country: in Oakland, California,

all equipment and tools for surveillance must now be approved by an oversight committee led by citizens before they can be implemented. If you're interested in learning more, you can check out the talk I gave on this at The Eleventh HOPE (2016). However, I must apologize that I haven't gotten around to writing an article on how we did that. The thing is, there are a lot of problems to try to solve and each individual can only do so much.

Speaking of individuals, let's talk about Milton Friedman. It's true that he created a very compelling documentary/interview series in 1980 called *Free to Choose*. I do recommend that everyone watch it. But I also recommend the series to which it responds: *The Age of Uncertainty* by John Kenneth Galbraith. Ultimately, a lot of this boils down to the economic debate between the Frankfurt School (Adorno, Marcuse, etc.) and the Austrian School (von Hayek, von Mises, etc.). It's a deep, complex debate that is not going to be solved in the pages of this magazine, nor is it a good idea to declare victory before addressing every issue within. For example, if Friedman's theories are so sound, then why did Paul Volcker's adherence to them tank the economy in 1979 when he was chair of the Federal Reserve?

To bring us around to the last point I want to address: Volcker was also an associate of Ayn Rand, who wrote *Atlas Shrugged* (and *The Fountainhead* and a number of other works). You'll recall from your readings that Rand admired strong men like John Galt and Howard Roark, who stood strong in the face of obstinance and "looters." But remember that her work is fiction: after all, it's hard to imagine *any* speech captivating an audience's attention for three hours, let alone John Galt's speech. It seems to me that her philosophy is in many ways an angry response to her childhood being destroyed by the Bolshevik Revolution. And I find it telling that she often claimed that the most important philosopher was Aristotle, who warns in his *Nicomachean Ethics* about the dangers of extreme vices and virtues. If she were actually a student of Aristotle, might she have tempered her views a bit? Maybe her friend Murray Rothbard had a point in his play *Mozart Was a Red,* which lampoons the Manhattan social club she curated.

In conclusion, while I do agree that taking a holistic approach is important, I would suggest to focus the lens on the community, rather than a given individual or two with whom you disagree. Engaging in these disagreements in a civil and respectful manner is how the community stays together.

aestetix

Inspiring such thoughtful dialogue is definitely a service to the community and something we need to do more of.

Dear *2600*:

In 40:1, DCT's article seems from the first paragraphs that it will be critical of specific topics or authors in *2600 Magazine*. It does start out that way, and includes some well-worn criticisms of the editorials touching on political issues, and of in-person meetings requiring COVID-19 vaccinations.

Overall, though, the article is one of a type we often see in the pages of *2600:* observations about the world's issues (political and otherwise), and some thoughts on where it might be worthwhile to focus efforts to educate or otherwise improve the situation.

Many of the topics in the article are talking points typical of MAGA or other political discourse. The author presented them in the context of hacking and more specifically *2600 Magazine,* and I have no objection to such views being included in the magazine.

My experience of *2600* is that it's open to a variety of viewpoints, and doesn't shy away from being criticized. This article demonstrates that openness.

Estragon

We would be quite upset if we weren't being criticized. And bored, too. If done in a respectful and calm manner, opposing views can be the vehicle in which we build our arguments and understand why we believe what we do, rather than simply following others and repeating their talking points.

Dear *2600*:

I write in regards to both the opinion piece by Delta Charlie Tango and the letter by Shaun in 40:1 who protested about the political content in *2600*. Clearly neither of these writers have been reading *2600* for very long.

Certainly they were not reading in the late 1990s when *2600* was the only paper you could find in Barnes and Noble even mentioning East Timor, let alone giving a full throated endorsement of independence. They may not have been reading in the years 2001 through 2004, when patriotic fervor still covered for all manner of national security innovations, which 20 years later would be dusted off and wielded by actors significantly less subtle in their use than their predecessors.

Hacking and politics - yes, mostly progressive politics, but politics all the same - have openly existed hand in hand since Abbie Hoffman's *Steal This Book* in 1971, and yet further back still. I recommend Phil Lapsley's excellent *Exploding the Phone* to both of the mentioned writers for the crucial historical context they appear to be missing.

xarph
408 area code

And for one more longer bit of feedback on that article from last issue, read the piece entitled "Giving a Damn" in the current issue. Thanks to everyone who wrote in with their thoughts.

Meeting Updates

Dear *2600*:

After several months in Raleigh, North Carolina with two or fewer attendees, there was some concern that our meeting was going dormant again. However, we had four show up for the March meeting, so we are still clinging to life.

arcane

It's so important to keep trying and to be consistent. You never know when someone from out of town will stop in or when a new person will finally make it to the meeting site. Having a website or Twitter handle makes it easier to communicate with future attendees. And to those who find themselves in a city with a meeting on a first Friday, you almost certainly won't regret stopping by.

Dear *2600*:

I would be excited to start a meeting in my area, but I have a couple of questions:

1) What usually happens at the meetings?

2) What are good places to have the meetings? Like a Starbucks or a park?

3) What do you usually bring to the meetings? I live in Anaheim, California near Disneyland.

Any help would be appreciated. Thanks.

saltine cracker

You really should attend some meetings in other places before starting your own if you're unfamiliar with how they work. You're fairly close to the existing Los Angeles meeting, so we suggest dropping by there first and then deciding if this is something you'd be interested in starting in your own area. To answer your questions, meetings are actually more like gatherings where people converse with other attendees, show off technology, make contacts, or just chill. There is no agenda. The meetings work best in public spaces where anyone can drop in, nobody is excluded, and people can leave without fuss whenever they choose. Food courts tend to work well. As to what to bring, anything that might be of interest to a hacker is great, whether that's a new or old gizmo, reading material, or cool hacker-related clothing.

Dear *2600*:

Howdy! I'll be attending the Phoenix event and I would like to present. I read it's "open" but my presentation is likely best served with a PPT. Can/should I present a PPT? If so, what do I need to ensure I can properly present (is a projector available?) otherwise I can just do verbal and can articulate well enough. I can share the TXT elements of my presentation I'd like to share if you want too. Thoughts?

"The WAF Guy"

This is way more preparation than meetings require. While some may indeed have the facilities for presentations, this is not something that's the norm, nor is it a requirement for any attendee to pay attention. We suggest contacting the Phoenix group directly through their website (phx2600.org) or Twitter handle (@PHX2600).

Inquiries

Dear *2600*:

I have read about some "inconvenient truths" that you guys are going through turbulent times and came to your website. Do you have a Patreon, GitHub sponsorship, or something similar? Could not find such a link on your page.

Let me know if there exists such an online recurring donation account of yours.

Ernst

We haven't gone down that road as of yet, but it's always a possibility if the situation devolves further. We shall see.

Dear *2600*:

I was wondering if you would be interested in a series of articles detailing cassettes, how data was stored on them, as well as how they work. I got into the hobby a few months ago after buying a portable dictation-type machine. A boombox later and I want to share my knowledge with the community. But I also feel this might be a subject touched upon before, so I want to confirm with you guys before I slave away.

luRaichu

We're not aware of an article on this subject and we'd be most interested in seeing one. For those who don't know, cassettes used to be a method of copying and storing software on early personal computers. We wouldn't be at all surprised if there were still people making use of this method somewhere.

Dear *2600*:

Bought a one-year subscription based on a suggestion from a coworker. Loved every issue I got since then. Saving up for a lifetime subscription, and I did the math! After 8.5 years, it pays for itself! Thanks to every hacker, past, present, and future for making this an invaluable resource for the digital frontier.

P.S. Dumb question, but what issue did Angelina Jolie's character have on her desk in the movie *Hackers*?

Ted

We don't have the time to go through the film to find this out, but it's likely to be an issue from the early 1990s as that's when filming took place. We can say that the scene where the FBI agents in the car are reading "The Hacker Manifesto" (written by The Mentor) from one of our issues is inaccurate since we never actually printed that. We believe this is what is called artistic license.

Dear *2600*:

This week my job announced an app for staffing and said that we could download it to pick up shifts. I guess not many of us did. So we got this group text saying that it was a mandatory download now. Your employer can't force you to download an app, right? I've never heard of this app or the company; it sounds sketchy. It's not necessary for the execution of our job duties.

L

They absolutely cannot require you to download anything onto your personal phone. If it's a phone that they supply, that's a different story. And there are many ways you can contest this should it come down to it. Maybe you don't even have a phone. Maybe you have an old flip phone that doesn't run this app. Or maybe you have a BlackBerry. Conformity is every manager's dream but it so rarely works and it's really easy to derail. Have fun.

Dear *2600*:

Do you have a mobile website?

Anderson

Interestingly, our machine is on wheels, but that's probably not what you meant. We try to make our site look good (or at least acceptable) on as many platforms as possible including mobile devices. If you're aware of any lost functionality there, please let us know and we'll try to improve.

Dear *2600*:

This is entirely hypothetical and I don't want to anger anyone. Please note I am not selling anything, I just need advice... but if I had, say, 15 plus years of *2600* magazines from the early aughts through approximately 2017, how would you recommend I get them to someone who will appreciate them? Should I keep them together or split them up? Can't give them away, but I'm not sure a spot like eBay is the best outlet. I just really want to make sure I find the right person to take this off my hands and am unsure what methodology would be best. I feel weirdly protective over things that are sentimental, but I desperately need to yeet some of my various collections before moving again. Thank you kindly for your advice!

Erika

There's no need to be so trepidatious. It's perfectly fine to sell your back issues if you feel the need to. Use whatever site allows this sort of transaction and let the buyer decide if they want to buy them individually or as a collection. And you should probably sell them for less than we do if you want to give people a reason to go to you instead. This is especially true if the issues are worn.

Dear *2600*:

Do you know your phone reads your face constantly on dating apps? This biometric algorithm allows social media algorithms to "rank" you. These ranks that are strictly made from your face are pretty dystopian. The ranks are things like attractiveness, trustworthiness, intelligence, responsibility, sociability, and race. This just doesn't work if you want to create lasting relationships. First of all, filters exist. What ends up happening is that only the most conventionally attractive or good-with-filters (arguably the most insecure) get to be seen. Unrealistic expectations are created in real life.

Tinder and Bumble are notorious for abusing this. What they like to do is give each user their scores and only show them their hottest options. This guarantees bad date after bad date. They keep the user on the app to cycle through the 9/10 to 10/10 meat market in hopes of a miracle. All in all, there are better ways to meet people.

X

Almost any other way is better. Superficiality isn't the answer. Our imperfections and faults are actually the most interesting elements in many cases. We'd like to see a dating app that focuses on those.

Dear *2600*:

The movie *Hackers* came out just before my 15th birthday, and it holds a special and nostalgic place in my heart. Repeated viewings after purchasing a VHS copy back then prompted me to develop a more critical and curious way of interpreting the world around me, as well as take a genuine interest in the technology of the time.

I've heard in passing that your editor-in-chief Emmanuel Goldstein worked as a consultant on the film. I was wondering if he's ever committed to paper what that experience was like and, if not, would he consider doing so in the future? As a die-hard fan of the film and a newly minted lifetime subscriber of *2600*, to say I'm interested in his musings on the subject is an understatement.

DL

It's an interesting idea which a few of us could contribute to. While there aren't any really major revelations, everyone involved seems to agree it was a smooth and pleasant production and every member of the cast was great fun to work with, as were other members of the team, from the writer to the director and many others. Of course, nobody really anticipated what a special place this tale would occupy in the hearts of many for so long afterwards. We're glad to hear it means this much to you.

Dear *2600*:

I am trying to download the old HOPE panels (I got a new iPod and I am wanting to re-download them since the hard drive I had them on died long ago), and a lot of the sites are down, or the link to stream/download the panels is down. It is not all of them - HOPE X seems to be working - but Beyond HOPE, H2K, H2K2, a lot of the earlier ones, are appearing to be down.

Robert

Every one of our recorded talks is on our YouTube channel (Channel2600). You can use a program called youtube-dl to capture either the video or audio from each of them. Of course, Google is often overaggressive in removing content it deems objectionable or in age-restricting talks based on antiquated morality settings, which is why everything is also available directly from us at store.2600.com completely uncut and uncensored.

Dear *2600*:

I have a digital subscription and enjoy the articles. I was wondering if you'd consider licensing a "re-print" option i.e., allowing me to post some of the articles in our internal intranet. It would be limited to a subset of our employees that are interested in IT security topics.

I think the writeup in 38:2 titled "More Privacy and Better Security Through Email Diversification" would be a great addition to our security awareness program. How much would it cost to get approval to reprint this article online in our intranet?

I would consider this first article a proof of concept. If our employees show more interest, we might be looking at licensing additional articles from you.

We certainly would be linking back to your website, and there is a good chance that some of our employees - who haven't heard of *2600* - might be subscribing to the magazine.

I appreciate your feedback - thank you.

Simon

You're welcome to do this without permission or compensation. As long as you're not charging for the material or redistributing our entire publication, we're OK with it. We do ask that credit to both the magazine and author(s) be given, as well as any possible encouragement for people to subscribe. But our main goal is to get the info out there and, for that, we thank you for your help with those efforts.

Dear *2600*:

I was told by a crypto-anarchist that the only way to get true anonymity in communication is to use a high-latency store-and-forward network. The individual I spoke with did not know of any networks that fit the bill. Are you aware of any such projects?

Odin

This type of a system is mostly used when the receiving party isn't available or reachable. We're not aware of any security advantages. This kind of thing was common in the past using systems like UUCP and FidoNet to deliver email decades ago. FidoNet actually still exists and we'd love to print an article on how it's being used in the present day.

Dear *2600*:

I was just reading 38:1 and I noticed that the mailbox in the cover image says "DAN" on it. That's my name! So I must ask, why did you choose to put that on the mailbox? There must be some meaning behind it.

DanN

Yes, there usually is some meaning behind our actions. In this case, it was a tribute to our late friend and hacker extraordinaire Dan Kaminsky, who had recently passed away.

Follow-up

Dear *2600*:

I previously sent you a letter asking why the MOTD on your IRC servers had a quote about the importance of firearms credited to C.S. Wheatley. You answered in 39:4, saying that the quote you see there now is a different one attributed to Benjamin Franklin. And you're right, that's what I see there too.

But the Internet doesn't forget, so I dug around and found this website (netsplit.de) that acts as a directory and search engine for IRC networks. I looked for 2600net, but it already showed the new quote. That's when I decided to use the magic of the Wayback Machine by the wonderful Internet Archive and found a few captures of the netsplit.de page where the previous quote was visible. It was there at least since 2020 and until October 2022. I'm sure it's been there for way longer, but the first capture by the Wayback Machine is from 2020.

You can see all captures at: web.archive.org/web/20200813031854/https://netsplit.de/networks/2600net/

Here is the quote:

"Firearms stand next in importance to the Constitution itself. They are the American people's Liberty teeth and keystone under Independence. The church, the plow, the prairie wagon, and citizens' firearms are indelibly related. From the hour the Pilgrims landed, to the present day, events, occurrences and tendencies prove that to insure peace, security and happiness, the rifle and pistol are equally indispensable. Every corner of this Land knows firearms and more than 99 99/100 per cent of them by their silence indicate they are in safe and sane hands. The very atmosphere of firearms anywhere and everywhere restrains evil interference and they deserve a place of honor with all that's good. When firearms go all goes, therefore we need them every hour." -C. S. Wheatley

Once again, why did you have that quote there? It doesn't seem to be fit for today's world but then again, I'm not an American.

Tiago

Thanks for doing the research on that. As the IRC servers are run by others not on the magazine's staff, we can only speculate that this represented one of the admin's opinions, in much the same way that people organizing meetings or running other online forums might have different perspectives on certain issues. There are things we might say here that would not wind up being equally represented in those places and the reverse is also true, those words being a good example. And, as the quote appears to come from 1926, saying that it "doesn't seem to be fit for today's world" isn't an unreasonable conclusion to reach. What's important here is to realize that the various individuals and groups working with us have different opinions, but also have common goals. It's not our place to expect people to agree with us on everything and we hope that readers, users, attendees, etc. will never feel as if their thoughts or perspectives don't matter or are being stifled.

Dear *2600*:

In 38:3, fux0r feels obligated to warn our community about the "horrific" "pedophile" in our midst. As an abolitionist and criminal justice activist, I now feel obligated to warn our community first against the use of socially charged but legally meaningless verbiage, and second of how easy it is to receive such a charge or conviction. All too often, sex-related charges have been used to discredit and destroy activists and community organizers. Julian Assange and the creator of the 3D-printable Liberator handgun are two prominent examples.

Two caveats to start: First, as a feminist, I do not wish to discount all or any victims of sexual violence or exploitation just to point out that the weaponization of such charges predates the #MeToo movement. Second, I do not claim to know, nor do I wish to explore, the specifics of the case fux0r brings to question - it may be valid or it may not. That is not for us to judge. That said, let's look briefly at three absurd examples.

Around 2017, two defendants are accused and convicted of Possession of Child Pornography with Intent to Distribute. They are a boyfriend and a girlfriend, ages 15 and 16. The pornography in question consists of private pictures sent to *each other*. They will both be labeled pedophiles.

A young man of 21 is convicted of Sexual Assault on a Minor. His "victim" is his girlfriend of four years, his "high school sweetheart." She testified on his behalf. Her family decided to press charges after "she" came out as trans and gay. The two young men have been happily married for nearly a decade. One of them is now labeled as a pedophile.

A young lady buys a fake ID to get into a 21+ nightclub. She is under the age of consent but looks of age. She buys a young man some drinks. Later, they have sex. Later still, she gets scared she is pregnant and her mother finds the test. Long story made short, the victim of her lies and her forgery is now labeled as a pedophile.

Let me ask you this, my fellow hackers: whose behavior here is "horrific?" Seeing how the records of cases involving minors are sealed to protect the minors, we cannot know if the person in 38:1 has "horrific behavior" or is simply the victim of our "criminally injustice" system. I strongly encourage each of you to look into the largest prison-industrial complex in the world, the school-to-prison pipeline which feeds it, and the convict slave labor which sustains it. All right here in the "land of the free."

Hack the Planet.

The Abolitionist

Regardless of the specifics in any particular case, the types of crimes people are charged with, or the very real horrors that victims of assaults must live with for the rest of their lives, we cannot deny that there are a whole host of miscarriages of justice where people are locked away for things they didn't do or labeled in an unfair manner either as a result of a corrupt prosecutor, lying witnesses, or bizarre laws. The fact is we simply don't know. And it's for that reason that we don't pass judgment on incarcerated individuals seeking to take out ads in our Marketplace, which is what the original letter writer was upset about. We do have standards and lines that we won't cross. But to cut off access to our own pages based on rulings we have no way of verifying and to treat them as a non-person would be Orwellian

and hypocritical for us, especially when we've seen the system abused so many times. We will repeat what we've said before: people need to exercise caution whenever they contact anyone they don't know. This holds true both for people who are incarcerated (where it's relatively simple to find their criminal history) and those who are walking around free who may have very ulterior motives.

Dear *2600*:

Back in Volume 26, William R. Epp wrote in "Dear *2600*" that 2600.wrepp.com was live and searchable. Since then the *2600* Index had a few mirrors and during the time I utilized it was updated to Volume 35, Number 3 (Autumn 2018).

Seeing the mirrors slowly disappear and no further updates made, I reached out to William to see what could be done. Initially, I wanted to create a new project under a new format, but as I continued to use William's site locally, I realized the best thing was to place it somewhere like GitHub where his open source Copyleft code could live on.

I've set the stage and, while it may remain in the current state for a bit, I have some ideas for future updates, such as including a "code" repository. There are questions there, of course, in terms of whether code from the *2600* Code Repository could be placed on GitHub, or if "new" files with the code examples from the magazine should be created as some have done. All questions for a future time, I suspect.

With a local copy of Apache and MySQL, using phpMyAdmin, it took less than five minutes to import the schema and data and start using the website locally. Until I started using William's site, I didn't feel a need. Now I'm starting to appreciate the work that went into it and have found it of great use.

I'm a shite community leader and evangelist, but I'll see if I can't get some interest going.

Chris

We wish you luck. FYI, the link you sent us didn't work, so this project may have already hit some roadblocks. We'll update as we hear more.

Dear *2600*:

Hi Unknown Unknown

I was wondering if you got a chance to review my previous email. Please suggest if there is any update for us.

I would highly appreciate your acknowledgment and valuable comments on my last mail.

I'm looking forward to your reply.

Kind Regards,
Bailey Borden
Business Development Executive

Well, here's the acknowledgment. Let us also advise you that if you're attempting to reel someone in to buy whatever it is you're trying to sell, addressing them as "Unknown Unknown" isn't the best strategy. The fact that this is a follow-up to a previous unsolicited email makes this even more worthy of recognition. And, still more amazingly, there was no website or company name mentioned here, just an email address that we're not going to give free publicity to.

Dear *2600*:

I'm on the code page: www.2600.com/code/ but I don't see any listings newer than Autumn 2017.

Eric

Yes, you would be correct in that assessment. Things have been real busy, but it's on our list, really. Maybe it will even be updated by the time you read this.

Dear *2600*:

I am submitting an attached draft of an article for your consideration in an upcoming issue of *2600*. I apologize because the text is slightly longer than the required 1000 words, and I remain at your disposal for any suggestions you may have.

G

We're curious how you were given the impression that articles shouldn't be longer than 1000 words. We actually like longer articles that go into more detail. Many is the time we've received articles that make us cry out in frustration because they end far too soon and leave us wanting more. Of course, if you've run out of things to say, you should probably stop writing. But please don't shorten your submissions to the point where you're leaving out material our readers might find interesting. And for anyone who is considering writing an article and getting all the free stuff that comes with that, the address is articles@2600.com. Guidelines can be found in the "Submissions" section of the 2600.com website or in ads found in every issue.

Preparing for Disaster

Dear *2600*:

I have a book called *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath* by Ted Koppel. It is about the possibility of a scenario where the electrical grid has been brought down by a cyberattack and there is a blackout lasting months or longer across several states or more. No running water, no sewage, no refrigeration or light. Scarce food and medical supplies. Banks no longer functioning, widespread looting, and law and order stretched to its outermost limits.

The book jacket says "It isn't just a scenario. A well-designed attack on just one of the nation's three electric power grids could cripple much of our infrastructure - and in the age of cyberwarfare, a laptop has become the only necessary weapon. Several nations hostile to the United States could launch such an assault at any time... 'It's not a question of if,' says Centcom Commander General Lloyd Austin, 'it's a question of when.'" And yet, as Koppel makes clear, the federal government, while well prepared for natural disasters, has no plan for the aftermath of an attack on the power grid.

I figure as *The Hacker Quarterly*, you must have some thoughts on these possibilities. As a result of reading that book, I have become what some call an "amateur prepper." I have extra bottled water and canned food, first aid supplies, survival books, etc. I would love to prepare a submission about my thoughts, fears, and preparations for cyber disaster/societal breakdown. My question is: would this be an appropriate submission for you? I would also love to hear readers' thoughts and responses if I were to write a submission and if it were approved.

Emily

Sure, that could be really interesting. We'd like to avoid the doomsday, survivalist angle and focus mostly on where the vulnerabilities are so that people can make up their own minds as to the best ways to be prepared for such a calamity. We're sure Ted missed some things.

Dear *2600*:

Could nanobots be denied quarter under the Third

Amendment? If the commander and chief of the armed forces orders nanobots into the home, such as in the case of biological warfare, are they considered soldiers? Under that interpretation, the Constitution would require nanobots be prescribed in a manner according with law. I take it that means Congress would have to pass a bill.

Henry

We doubt these nanobots would be defined as soldiers since that would make it easy to apply the Third Amendment against them occupying our homes. But they most certainly will be considered weapons. We honestly can't wait to see how Congress handles this issue.

Artificial Intelligence

Dear *2600*:

Has anyone's workplace prohibited ChatGPT's use, or that of any other type of generative AI? We just were told we have a temporary ban on any of these products, including Google Translate, while issues get sorted out. I think that is a wise precaution.

Norm

A blanket ban is simply panic. Such tools can be quite helpful if used in a responsible manner. Anyone who uses them for a while will soon become familiar with the writing style and other qualities that make it painfully obvious when artificial intelligence is being used. The amount of misinformation that is put forth as fact will actually wind up damaging the reputation of anyone who believes what a chatbot tells them without doing a good degree of factchecking. And if someone does indeed factcheck while being given possible solutions to questions by artificial intelligence, they're actually doing work instead of simply using this technology as a crutch. We've seen this before whenever something new and powerful is introduced. So banning isn't the answer. Education, experimentation, and due diligence is.

Dear *2600*:

We're nowhere near having artificial intelligence that will "end humanity" despite all the recent foreboding. ChatGPT is nothing but a glorified text analyzer/generator, a language learning model that works with probabilities. There's no "intelligence" in it. True intelligence is a function of sentience and that can't easily be artificially replicated. It's also possible that intelligence can't occur without sentience and this would require the use of biological material - the only known conduit for sentience - a technology that is very far into the future. We underestimate the role of sentience/consciousness in the process of decision making, a crucial component of intelligence. Robotics is also in its infancy and so a "takeover" of AI against humanity is science fiction. There's also EMP and microwave technology that can instantly stop electronics from transmitting. We're going to be fine and, no, we are not six months from "doom and gloom." The danger is that this AI precursor we have is *not* intelligent enough to make correct decisions, not that it is too intelligent. This is probably the reason behind the warning from Elon Musk, et alia.

LM

Although it is always nice to see the richest people in technology fall into a panic.

Stories

Dear *2600*:

At the dump yesterday, some woman threw a PC into the generic household waste dumpster. While the PC was sinking like the Titanic surrounded by black garbage bags, I said loudly, "You did permanently erase the data, I presume?" Judging by her face, I think I might have ruined her Easter.

Mike

That's truly evil. But educational too.

Dear *2600*:

Just a reminder that if your files are sitting on someone else's server, you have no control over them. I set up an Instagram account in 2014, followed a few people, but only uploaded my first pictures last month (a few landscape shots). I tried logging in today to find a message saying that my account had been suspended on the first of April and that to gain access I needed to supply a phone number. A quick check on Google indicated that the account no longer existed. I have no idea why it was suspended and I only had five photos uploaded, but I imagine this would be devastating to someone who had hundreds of photos and followers.

David

Absolutely. And it happens all the time. Whether it's because of some sort of violation of the company's rules (and they can really make that about anything they want), a crazy copyright issue, hardware failure, or the company itself ceasing operations, your data can very easily become inaccessible at a moment's notice. That is why it's essential that you have multiple places where the same data is kept and that you have local access to it in case there is some sort of a massive failure of the Internet. When services like Facebook come onto the scene, we mistakenly believe that this will ensure that all of our memories and interactions will be forever saved. But quite the opposite is more likely. Sure, individual photo albums and correspondence can be lost over time, but if literally billions of people store these items digitally and that entire system disappears for whatever reason, how many memories are forever lost? Another exercise to drive this point home is to ask people if they know where to find a family photo album their grandparents had. Many people are able to gain access to such a relic. However, when you ask almost anyone to show you pictures from their first digital camera - perhaps one of the very first back in the 1990s - they almost never know where those pictures wound up. Combining technology with old school methods of storage is really the only way our priceless memories can be preserved.

Thanks

Dear *2600*:

I just wanted to thank the magazine. I took your advice and filed a dispute on some old debt in a "holding action" per an old issue. I prevailed. Guess they didn't find their paperwork in time.

Paul

While we don't recollect exactly what we said, it sounds like something we'd advise. Always fight back and never accept someone else's facts without putting forth your own. We hope this inspires others to do the same.

Dear *2600*:

Holy crap, coming up on 40 years? I graduated high school in 1984 and let me tell you, I can't believe either of us is still around! Hacking has given me invaluable life skills. Forty years later and I still read the letters section first. I'll buy a digital subscription as soon as you have it worked out. Happy 40th!

Shelley

Thanks - it's been quite a ride so far.

Dear *2600*:

Oh man, this is still a thing! Haven't read *2600* in over a decade! Can't wait to start reading it again! Thank you, c00L d00ds!!

Marc

We get this a lot. What we're most curious about is where people go where they become unaware of us still existing before they come back and discover that we're still around. Regardless, it's always good to get reacquainted.

Random Thoughts

Dear *2600*:

I ran across your posting and it seemed interesting. I'm contacting your group to see if any of you get hired to confirm if a house is being hacked, along with all electronic devices in it. I know my house but need confirmation. Other agencies are looking into it, but are slow. Please let me know and if one of your members is willing, the cost to do so. Includes phone, security system, security cameras.

Joe

Friends, this is the future. Hacked houses where everything within is compromised: microwaves, refrigerators, doorbells, furnaces, air conditioners, washing machines, you name it. Not one of those devices needs to be connected to the outside world, but many of us will either bow to the temptation or get hoodwinked into buying a product that gives you no choice. Of course, as your letter demonstrates, this opens up a whole world of opportunity for people looking to fix these mistakes and repair the damage.

Perhaps we should point out here that we have no idea what "posting" you're referring to and that this is not the kind of thing we're involved with. Maybe something else got hacked to create this impression. We'll need to hire someone to fix it.

Dear *2600*:

I am writing to you to address a word. Not a fixed-size group of bits, sadly, as might normally be the case, but rather a discrete unit of language that holds particular meaning.

I have conferred with the foremost among the experts, and I have indisputable, incontrovertible, purely-objective-mathematical-proof that you have been using this word in error. Many tactful and intelligent (and handsome) writers have spoken out about your vile use of this certain verb, and have accused this publication of the misdeed - the twisting, deceitful jab - delivered by this repeated utterance. I am inclined to agree with them, although none have yet supplied natural-historic demonstration as I shall presently.

Feel free to fall to your knees and grovel at my feet once you have seen the folly of your ways while the brilliance of my intellect burns away the fog of ignorance that ensconces your feeble minds.

You will notice that the foremost publication in the history of the world (www.worldhistory.org) refuses to use the term. They have not as of yet responded to the list of demands I have nailed to their door, but I have a theory:

You see, they never use the term "defenestration" in referring to the unfortunate events of 23rd May, 1618 AD. The Wiktionary Czech-to-English dictionary defines the Czech word "defenestrace" as "defenestration," which it then specifies as "(act of throwing out a window)."

You see, typical windows in 17th century Bohemia, as in all places, are elevated above the ground, but are *not* particularly high. About waist height for the typical person.

Only a fool would think that the rabble could convey the four Catholic Lords Regent et al. through such a window by *lifting*. The fact of the matter is that these stalwart defenders of the Papacy were merely pushed through the window, not thrown out.

To think that the radical Hussite weaklings could throw such men through a window is, on its face, ridiculous. Perhaps you can argue with the Wiktionary, but really, would you be so oafish and bullheaded to contradict www.worldhistory.org?

I submit this to you out of the immense regard I have for 2k600 as well as the deep sadness wracking the faithful masses who plainly see through your deceit and Protestantism. QED.

Warmest Regards and Kisses,
and May You Rot in Hell,
Sir Tinley Aninsell

We may never know what prompted this. And we have to accept that.

However, the writer is in error concerning the non-use of the phrase "defenestration" with regards to the Bohemian Revolt on www.worldhistory.org. On that very site is this quote:

"The Bohemian Revolt began when Protestant nobles, led by Count Thurn (l. 1567-1640), objected to legal decisions favoring Catholics and met with three of Ferdinand II's representatives at Prague Castle to discuss the situation. Unhappy with the proceedings, Thurn and his colleagues threw the representatives out the window in what has come to be known as the Second Defenestration of Prague (the First Defenestration being the event that began the Hussite Wars)."

So there.

Dear *2600*:

Tried to join the Facebook group to gain some insight into significant cyber breach experiences. I was basically told hackers don't assist with this type of gig? Throwing people under the bus comment, which I have never done.

Per your website, looks exactly like what you do, perhaps unethical hacking there in New York.

Sweet. No thanks. I'm the good guy.

Lisa

We honestly have no idea what you're referring to. First off, we have three Facebook groups, all run by different people with only very loose affiliations with the magazine. What someone tells you on one of them may not correspond with what we would tell you in these pages. That's the nature of the hacker world. If your request there was as unclear as the words above,

we can understand why someone might brush you off. We don't know if you're trying to instigate or prevent a "significant cyber breach experience." Saying you're the good guy means nothing since that's what everyone believes of themselves. So, not knowing what it is you're trying to do, there's not much we can say. Other than you won't find much sympathy if you're looking for help doing something illegal or destructive. You also won't get many fans by trying to recruit people into some sort of hacking business. We suggest instead that you read the room for a bit and then start to converse with people in ways that they're clearly comfortable with. Jumping to conclusions about something you're just getting involved with isn't the best way to achieve anything.

Thoughts on the RESTRICT Act

Dear *2600*:

I urge any U.S.-based members to call their reps for their state/district and ask them to vote no on the RESTRICT Act. If allowed, it gives the government the power to ban any app or program with over a million users that use any type of foreign technology or programming. It also states that using or teaching how to use VPNs or other methods of circumventing such bans will result in a felony and a $250,000 fine.

Jeremy

This is yet another example of the cluelessness our elected representatives demonstrate when it comes to technology. This particular bill is being led by panic over TikTok and what the Chinese government might be able to do with data that popular app collects. While we should be concerned with such collection by any entity, this is so clearly not the way to go about it and we honestly can't see how this bill will ever become law. Still, that hasn't stopped the state of Montana from passing its own law banning TikTok. We have no idea how they think they can enforce this, but some of the legislation being passed by state governments recently has been both frightening and illogical. We can only advise that people fight back at every level. You have so much more power than you've been led to believe.

Dear *2600*:

There has been extensive public discourse about the RESTRICT Act (S. 686), which was proposed on March 7th, 2023. Some people seem to think that it's good, and that it will help ban TikTok. However, many people are concerned about the broad language that it uses, the sweeping powers that it grants to the Secretary of Commerce, and section 15(f) which explicitly states that the Freedom Of Information Act will not apply to this act. I have personally read the bill, and would like to call attention to a section that no one seems to be talking about, and that I find particularly concerning. Section 5(a) of the act details types of technology products and services that the Secretary will "prioritize evaluation of" (supposedly for the purpose of discerning whether or not they are a national security threat). Most of the specified technology areas are somewhat general, and could possibly be construed as being harmful for a foreign adversary to possess significant market shares in. However, section 5(a)(3)(C) gets very specific, and singles out "data science products and services, including those involving the provision of services to assist a party utilize, manage, or maintain open-source software." I find this to be a little weird. Are we really worried about foreign adversaries attempting to develop open-source software? In the cases that they do, such as the open-source parts of the KaiOS Linux distribution, do we really want to stop them? Wouldn't we actually want them to focus more on open-source so that we can more easily investigate their software? Personally, I am opposed to the RESTRICT Act. I am interested in hearing your thoughts on this issue, and would encourage anyone who's interested to read the full text of the bill on congress.gov.

Craig

It's so important to read every word of these bills (which is often more than members of Congress do) because little gems like the above are always hidden in them. We can laugh at the absurdity, but it's not particularly funny when such bills are part of an overall agenda backed up by politically placed judges who will sign off on anything the people who nominated them say. We'd like to believe the system doesn't operate like this, but a recent look at what's been going on in the courts will demonstrate how it all really works.

Dear *2600*:

The RESTRICT Act is evil. The RESTRICT Act not only bans Americans from using TikTok, it is a Patriot Act 2.0 for the Internet. It would give the government unfettered access to all the data on our computers, phones, security cameras, Internet browsing history, payment applications, and more. It throws the Freedom of Information Act out the window, cannot be challenged in court, and criminalizes the use of a VPN with up to 20 years in jail and a one million dollar fine.

Kevin

In case you're wondering why we're always capitalizing "RESTRICT," it's because those clever people in Congress named it the "Restricting the Emergence of Security Threats that Risk Information and Communications Technology Act." They always do this - the USA PATRIOT Act is actually the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act." If only the bills they introduce were as good as the acronyms, we wouldn't constantly be dealing with such idiocy.

While both Democrats and Republicans have stood behind the RESTRICT Act, we've also seen political opposition from both sides of the aisle, which is a good thing. Again, where it's particularly bad is on the state and local levels, where there often is only one side with power and where the feeling that they can get away with whatever they want exists. So it's vital to not only attack this nonsensical bill, but to also reverse the local pushes to accomplish the same thing and sometimes even more egregious attacks on our freedoms. We do this by paying attention and never backing down.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

EFFecting Digital Freedom

by Jason Kelley

Edward Snowden's Revelations, Ten Years Later

In 2013, Edward Snowden broke the Internet - or rather, revealed that the Internet was already broken. His disclosures about the NSA's secretive mass surveillance programs shook the very foundations of our thinking about online privacy and government spying. EFF and others had been working for years to reveal anything we could about the NSA's ability to spy on people's online communications, Internet activity, and phone records, both inside and outside the U.S. But the disclosures did more than just clarify what we suspected: after these revelations, we were able to better pinpoint our demands, our questions, and our legal tools.

We've had some big wins as a result. In 2015, the NSA ended its program of bulk collecting Internet metadata, including email addresses of the sender and recipient, and IP addresses. Senator Ron Wyden, a longtime digital rights advocate, and others who were granted access to the program under the limited congressional oversight that existed, helped kill this program (and ongoing pressure from litigation by EFF and others didn't hurt either).

Some of the programs Snowden revealed have sunset - like the dragnet surveillance program that collected billions of phone records documenting who a person called and for how long they called them. And we've been able to receive classified rulings (heavily redacted) from the Foreign Intelligence Surveillance Court (FISC), which give us some insight on how and when it grants surveillance powers to the government and the reasoning which guides its decisions.

And the wins after Snowden's revelations aren't all legal. Prior to 2013, much of the web was primarily served over unencrypted HTTP instead of HTTPS. EFF, along with many partners around the world at Let's Encrypt and elsewhere, created a baseline of privacy (and security) protection for people around the world by encrypting the web, which was spurred on in part by the revelations of the NSA's surveillance. Your support of EFF tools like Certbot and HTTPS Everywhere have helped us get there - over 90 percent of web traffic is now encrypted, and major browsers have deployed key features that put HTTPS first. You can tell how effective this campaign has been by visiting any of the rare sites still served over HTTP, and seeing that your browser reminds you this data is insecure.

But there's a lot more to do. In particular, we must end or at least radically reform Section 702, which is set to expire later this year. Under Section 702 of the FISA Amendments Act of 2008, the government can conduct surveillance inside the United States by vacuuming up digital communications so long as the surveillance is directed at foreigners currently located outside of the United States. Though the law prohibits intentionally targeting Americans, the NSA routinely ("incidentally") acquires innocent Americans' communications without a probable cause warrant. Once collected, the FBI can then search through this huge database by "querying" the communications of specific individuals.

The Snowden revelations gave names to two of the key types of surveillance that the NSA conducts under Section 702: PRISM and Upstream. It also made it easier for us to get data on just how many innocent Americans' communications are searched through these programs. In 2021 alone, the FBI conducted up to 3.4 million warrantless searches of Section 702 data to find Americans' communications through its "incidental" collections.

Section 702's authority persists to this day. We did have another big win when one type of data collection under Section 702 was paused in 2017: "About," as opposed to "incidental," collection, was the scooping up of information when a target is merely mentioned, instead of communication specifically sent to or from a target. If you email a friend in France and discuss a known terrorist, for example, the email could be included as "about" a target. This collection ended after pressure from FISC (surprisingly) and groups like EFF and ACLU, but much of Section 702's surveillance authority remained.

We still need to permanently end this kind of collection. But that alone isn't enough. We must end Section 702's surveillance powers entirely, or considerably reign in the NSA's backdoor data collection. Currently, Congress has to renew Section 702 every few years. It was last renewed in 2018 and is set to expire at the end of 2023.

This isn't a stale debate. A new FISC court order unsealed earlier this year detailed massive violations of Americans' privacy by the FBI, underscoring why Congress must act. That opinion showed that for years the FBI illegally accessed a database containing communications obtained under Section 702 and other FISA authorities more than 278,000 times, including searching for communications of people arrested at protests of police violence and people who donated to a congressional candidate. The FISC ruling points out that the FBI is incapable of policing itself when it comes to trawling through the communications of Americans without a warrant: "There is a point at which it would be untenable to base findings of sufficiency untenable on long promised, but still unrealized, improvements in how FBI queries Section 702 information," the court wrote. That point is now. Clearly, the FBI has failed to comply with even the most modest reforms designed to limit the agency's surveillance powers.

The FISC ruling itself shows that the Foreign Intelligence Surveillance Court is incapable of protecting Americans from the FBI's unconstitutional searches of their communications. The court has consistently approved and re-approved the agencies' ability to use Section 702. In this opinion, it recognized that "compliance problems with the FBI's querying of Section 702 information have proven to be persistent and widespread." Although the court suggested that further incidents might prompt limiting who within the FBI could access information obtained under Section 702, it imposed no other restrictions on the FBI besides those proposed by the agency itself.

If recent bills are any indication, many in Congress would be fine allowing FISC to continue offering these judicial rubber stamps. And it would be fine allowing "about" collection to restart, and not only reauthorizing Section 702, but moving the goalpost for it to sunset down the road six more years. That means now is the best opportunity for Congress to limit NSA surveillance. This year we must push Congress to protect our communications, and our privacy, by ending Section 702.

Next Level AI: ChatGPT

by Chat GPT and macmaniac

As a hacker, you're likely familiar with the concept of chatbots and their role in automating conversations with users. But have you heard of ChatGPT? It's a cutting-edge technology that has the potential to revolutionize the way we interact with machines.

ChatGPT, also known as Generative Pre-trained Transformer 3 (GPT-3), is an artificial intelligence language model developed by OpenAI. The technology is built on a neural network architecture and uses unsupervised learning to generate human-like responses to natural language input.

The history of ChatGPT goes back to 2015 when OpenAI was founded by tech giants like Elon Musk and Sam Altman. The company's mission was to create a more intelligent and beneficial AI that could be used for the betterment of society. To achieve this goal, they focused on developing advanced language models that could understand and respond to natural language input.

In 2020, OpenAI launched ChatGPT, which quickly gained popularity due to its ability to generate natural-sounding text that is difficult to distinguish from human-written content. The model was trained on a massive dataset of over 45 terabytes of text, including books, articles, and websites, making it one of the most advanced language models available.

One of the most significant opportunities offered by ChatGPT is its potential to transform customer service and support. With ChatGPT, businesses can automate their customer service and support functions, providing customers with instant access to information and support without the need for human intervention. This can lead to significant cost savings for businesses and improve customer satisfaction by providing faster and more efficient support.

Another opportunity for ChatGPT is its potential to revolutionize the field of content creation. With its ability to generate high-quality text, ChatGPT could be used to create written content for websites, social media, and other digital platforms. This could save content creators a significant amount of time and effort while also improving the quality and consistency of their content.

However, as with any new technology, there are also risks associated with ChatGPT. One of the most significant risks is the potential for the technology to be misused for malicious purposes. ChatGPT could be used to create fake news, propaganda, and other forms of disinformation, which could have serious consequences for society.

Another risk is the potential for ChatGPT to perpetuate existing biases and stereotypes. The technology is trained on a massive dataset of text, which could contain biases and stereotypes that are present in our society. This could result in the model generating biased or discriminatory responses, perpetuating the very problems that we are trying to solve.

To mitigate these risks, it is essential to ensure that the development and use of ChatGPT are done ethically and responsibly. This includes carefully selecting and monitoring the data used to train the model, creating safeguards to prevent the technology from being misused, and regularly auditing the technology to ensure that it is not perpetuating biases or stereotypes.

In conclusion, ChatGPT is a groundbreaking technology that has the potential to revolutionize the way we interact with machines. Its ability to generate human-like responses to natural language input has numerous applications, including customer service and support, content creation, and more. However, there are also risks associated with the technology, including the potential for misuse and the perpetuation of biases and stereotypes. As hackers, it is our responsibility to ensure that the development and use of ChatGPT are done ethically and responsibly to maximize its potential for positive impact on society.

The article could end here. How did you like it? How did you feel about it? Did anything annoy you? Maybe something you can't really explain? It might not be a very original approach, but everything (besides the title) before this paragraph was written by ChatGPT itself! I don't have a lot of experience with it, just used it around four times for a question I was wondering how ChatGPT would answer to. This is to show you I am not an expert at all with ChatGPT. Nevertheless, it took me only about ten minutes to have the above written, of which I needed five minutes to realize ChatGPT got stuck in the second run. Here's what I finally asked ChatGPT in my third try (typos included) on February 18 2023:

Please write an article for a hacker audience, with a length of roughy 800 to 1000 words about the history of chat gtp, it's opportubities and also it's risks.

In a first attempt, I put the "hacker audience" at the end: "*[…] also it's risks for a hacker audience*." As I forgot the comma, ChatGPT started to write about the risks for hackers. Not what I intended, so I stopped ChatGPT and tried again. This attempt got stuck, but

my third attempt succeeded, resulting in the text above. So with relatively small effort, I got an article I could try to publish in *2600 Magazine*. From the beginning, it was clear to me that I wouldn't attempt to have this article written by an AI be published under my name.

Let's have closer a look at the text ChatGPT wrote. When I went through the text for the first time, it felt like it was written by the public relations department of ChatGPT. The AI is "cutting-edge," might "revolutionize" how we interact with machines. Its founders were "tech giants" and, in brief, it aims for a "betterment of society." It then points out the opportunities before talking about the risks. I wonder if it would have talked about risks if I hadn't specifically asked for it. But the risk is considered nothing special, it's just like "with any new technology." And - not having been asked for - ChatGPT also shows how these risks can be mitigated. The text as a whole is written in a rather positive language, containing expressions such as "betterment," "beneficial," "responsibly," or, well, "positive."

What I also noted is that ChatGPT took my given parameters seriously. The term "hacker" is the third word in the article. In the third paragraph, ChatGPT talks about the "history" before looking into opportunities and the risks. Where it did fail was for the length: it's only 576 words, and not between 800 and 1000. The single paragraphs are rather short, the conclusion being the longest with 91 words. This could be a hint on how ChatGPT generates articles: by writing single paragraphs covering a topic and then putting it together. Synonyms don't seem to be a thing ChatGPT is very good at. Not only does it repeat the given keywords, but also phrases: the twofold "ethically and responsibly" appears twice. For the second example of both, opportunities and risks, it chose "Another opportunity" and "Another risk." If there would have been a third risk, would it have been rephrased? Having examined only a single article, I cannot tell. All of the above needs to be verified with further research, eventually showing a clear pattern on how ChatGPT writes articles.

Me personally, I have mixed feelings regarding AI. On the one hand, it's a very fascinating topic, a technology people could benefit from. On the other hand, I'm rather skeptical towards new technologies that are praised or are being taken as a solution for whatever problem mankind has, as every technology can be abused. I clearly represent the opinion that scientists should think about and be aware of their invention's impact. Nowadays more than often new technologies are being welcomed, and criticism is dismissed as preventing progress. Progress and money making is most times regarded as more important than clean and functioning products, as the failures of the presentations of Microsoft's Bing AI and Google's Bard once again proved. Regarding AI and ChatGPT, I would suggest some guidelines to make it more trustworthy.

Every use of ChatGPT should transparently be declared. The consumer then is aware of the true authorship of the product and thus can contextualize and interpret it in a much better way. This actually should be the case for every written product but, unlike human authors, I doubt that ChatGPT would accuse anybody of plagiarism, or even be aware of being plagiarized.

ChatGPT itself should be aware of its sources. This is one of the big secrets: where does it get its knowledge from? One of the first thing scholars learn in university is specifying sources. You just don't claim anything, but you rely on other people's work, like thesis and studies, and you transparently declare that you used these works as sources for your own work. This also helps others to estimate the degree of your work's credibility. We had these issues already in the past: articles have been published anonymously by unknown authors or even under wrong names to hide the actual intention of a text. Nowadays with social media, fake news spreads much faster, and with technologies like ChatGPT it can be created faster and in better quality than it used to be. But the technology helps both sides: those who abuse it for creating falsified content, not only written, but also fake images or videos; and hopefully also those who try to find possibilities to identify fake content with the help of AI.

That's where we, the hacker audience, comes in. We strive for the truth wherever we can, and thus we should support and search for solutions to identify and fight forgery. We should put hands on ChatGPT. Figure out how it works. Try to make it do things it's not intended to do. Bring it to its limits. Figure out adversarial attacks. Show the risks. Turing test it. Abuse it (for the good). Break it. Talk about it. Use it. Test it. Hack it. That's what hackers do. I totally agree here with Chat GPT, that considers itself a hacker: *"As hackers, it is our responsibility to ensure that the development and use of ChatGPT are done ethically and responsibly to maximize its potential for positive impact on society."* What a nice phrase as a conclusion.

We are adding new hacker-related clothing items every month!
2600.store

Tomorrow's Challenges: Non-Fungible Tokens

by MadNinjaSkills

Non-fungible tokens have taken asset and art collecting into the digital world. This happened without clarification on the dangers of fraud and theft that can occur with such assets that are typically transferred through decentralized sources and without overseen provenance.[1] The decentralized nature of NFT transactions and lack of technical knowledge in the cryptocurrency space in general - with NFT marketplaces instead catering to massive consumer demand - can make those marketplaces liable for negligence.

To start understanding what exactly non-fungible tokens[2] [3] are, and what purpose they might serve, a person must first understand the definition of "non-fungibility," and secondly, what distinguishes a "cryptocurrency" from a "token".[4] Fungibility[5] is defined as the ability for one item to not stand out as unique or independent from another one. If someone buys a pack of gum with a five dollar bill, that five dollar bill will be perceived the same way as any other bill of the same value. The point is that by being "non-fungible," the token is defined as "rare," "unique," "one-of-a-kind," and "original;" and that scarcity is what theoretically drives the demand value of the NFT higher.

Next: What is a token? A token is a coin that predominantly utilizes a smart contract,[6] as opposed to a cryptocurrency that is used strictly for standard monetary transactions like the on-chain lightning layer of bitcoin - or like bitcoin that is frequently used as a store-of-value (as cited by MicroStrategy CEO Michael Saylor[7]). A smart contract basically serves a purpose on a specific blockchain that is superior to a transactional or commercial value. Here's a non-digital analogy to a smart contract: If a person puts money into a parking meter, they're basically creating a non-digital version of a smart contract in that they're paying for the purpose of parking for an allocated amount of time. "Tokens" differ from "cryptocurrencies" in that tokens descend from the native cryptocurrency of a blockchain that covers the token's transaction fees - and also the tokens are executing smart contracts instead of primarily executing basic commercial and transactional methods of exchange.

The first major boom or "bull run" of NFTs began with the graphic artist Beeple (Mike Winkelmann)[8] selling his NFT artwork "The First 5,000 Days" at a Christie's auction for more than 69.3 million dollars. When asked by *Business Insider* if there's any reason why people should pay a staggering amount for a work that might be downloaded as a .JPEG image, Beeple agreed, "Well, that's not a totally invalid argument." He said earlier in the interview, "We value things so that if everybody wants them, they have value. I mean, like, what makes a Louis Vuitton purse have value? It's just a brown leather purse. [...] So, it's sort of like saying, 'Do you think a web page has value?' Well, I don't know. It could be."[9]

This makes a ruling like *Shaw v. The United States* more difficult to acknowledge because "value" is made entirely subjective. Even film director Quentin Tarantino questioned how NFTs could at all supersede the value of the original posters and .JPEG images.[10] When he launched a campaign with the Secret Network to auction NFTs inspired by his film *Pulp Fiction*,[11] Miramax immediately blocked the sale under the claim that the company held the film's rights - bringing the notion of NFT's alleged immutable trademark and/or ownership under scrutiny.[12] What became of the NFT "ownership" received by many bidders who spent more than several thousand dollars of cryptocurrency each for Tarantino's NFTs? They received no NFT ownership whatsoever.[13] With this instance of trademark being very vague and inflexible, even NFT artists with honest intentions can find themselves in civil court when in a similar situation because there are no checks and balances for trademarks on NFTs yet that are already in place for things like musical albums, films, or book series that are protected in an official capacity by entities like the U.S. Patent and Trademark Office. The ecosystem of NFTs is so new and the concept of what an NFT "is" as an actual medium is so vague and unformalized that it would be easier for "patent trolls" to stop the sales of certain NFTs without there being a clear uniform definition for what an NFT actually is under U.S. law and actual legal protections and consequences in place for NFT artists, distributors, and buyers.

The main takeaway is that the U.S. judicial system finds it difficult to create constant

legislation and/or consumer protections for cryptocurrencies and digital tokens because neither falls under property that can be protected such as property that qualifies under *in rem* or even *quasi in rem* jurisdiction. The digital assets are peer-to-peer[14] so, with or without government scrutiny, their economic flow is mainly under the watch of normal citizens (as opposed to the FCC monitoring broadcast transmissions or the IRS evaluating a source of cash flow). The assets are well known for their extremely brief transaction period (as opposed to having to wait a few days for a wire payment to go through or a stock sale to settle)[15] as well as their portability (since the assets are a cumulation of ones and zeros that have substance and form when they're pulled up on a hard drive or a smart phone - as opposed to gold coins or bars of palladium that are more difficult to transport[16]). Both of these factors have allure in the cryptocurrency space because it makes the digital assets harder to seize in case an individual wants to hold onto them for the long term. The drawback is that without knowing how to legislate assets that do not take a clear three-dimensional shape and form,[17] it's very difficult to protect digital asset consumers who mean well when they have any instances of theft, malice, or manipulation to cope with as a result of investing and dabbling in digital assets. The IRS has regularly taxed digital assets - cryptocurrencies and NFTs - as property.[18] Despite the U.S. government's inconsistent feelings towards cryptocurrency and difficulty with it in the past, it has been able to profit off of the cryptocurrency space.[19] [20]

For everyone to not be manipulated into purchasing counterfeit saved .JPEGs or .AVIs of NFTs on the secondary market, they can just analyze the trademark and copyright metadata imprinted on the blockchain from the transaction listing on the etherscan.io website.[21] The problem is that most of the people in the NFT space don't know how to inspect a smart contract[22] [23] [24] or what to look for on the transaction history on EtherScan.[25] An attacker can easily create a duplicate NFT marketplace[26] [27] and use a malicious constructor[28] in the smart contract attached to their fraudulent NFT to create a backdoor in the victim's wallet and steal all their cryptocurrencies and NFTs. What's worse is that the imposter can store the victim's NFTs on a hardware wallet like a Trezor wallet and then the victim can't get those original artworks back and is out of money.[29] Plus it's harder for the courts to prosecute because they'd need to know where the hardware wallet is that uniquely signs for the execution of the transaction and force the attacker to return the NFT to its rightful owner.

By creating a marketplace for NFTs with no awareness of legal consequences, NFT markets are opening themselves up to major scrutiny. When it comes to collectible NFTs, some of the technological foresight of the users could probably be presented if, for example, "The user must be running their own node."[30] [31] This would provide less liability for that NFT dealer in similar ways that investors are required to have a certain amount of capital to start investing in specific highly valued assets on E-Trade or Fidelity. That user would also be likely to be more technologically adept with the subjects of NFTs and cryptocurrencies. Also, legislation against celebrities heavily endorsing technological projects they know nothing about might help.[32] [33] The legislation would be similar to "money transmitter"[34] requirements that have been used against individual buyers and sellers of cryptocurrencies who acted as if they performed business in an official capacity such as the kind a CPA or other licensed official would. Also, something should happen to introduce how smart contracts ought to be treated in the courts, since they are not treated as officially binding legal contracts. Even if NFTs are only a bubble that might not garner the same attention in the future, non-fungible tokens may have introduced the legal and judicial systems to new advancements in the contexts of blockchains and smart contracts that were very necessary for technological legislation to progress into the 21st century.

References

[1] "$1.7 million in NFTs stolen in apparent phishing attack on OpenSea users", *The Verge* ; Russell Brandom - Feb. 20, 2022 ; www.theverge.➥com/2022/2/20/22943228/opensea-➥phishing-hack-smart-contract-bug-➥stolen-nft

[2] "What is an NFT? Non-fungible tokens explained", *CNNBusiness*; Jazmin Goodwin, Nov. 10, 2021; www.➥cnn.com/2021/03/17/business/what-➥is-nft-meaning-fe-series/index.➥html

[3] "Non-fungible tokens (NFT)"; Ethereum.org ; ethereum.org/en/nft/

[4] "What's the Difference Between a Cryptocurrency and a Token?"; Parker McCurley, July 18, 2019; Medium.com ; medium.com/decentlabs/➥whats-the-difference-between-➥a-cryptocurrency-and-a-token-➥e7c3b3226527

[5] "Moneropedia: Fungibility" ; www.getmonero.➥org/resources/moneropedia/➥fungibility.html

[6] "What Are Smart Contracts On The Blockchain and How They Work" ; Jake Frankenfield, March 24, 2022; Investopedia.com ; www.investopedia.➥com/terms/s/smart-contracts.asp

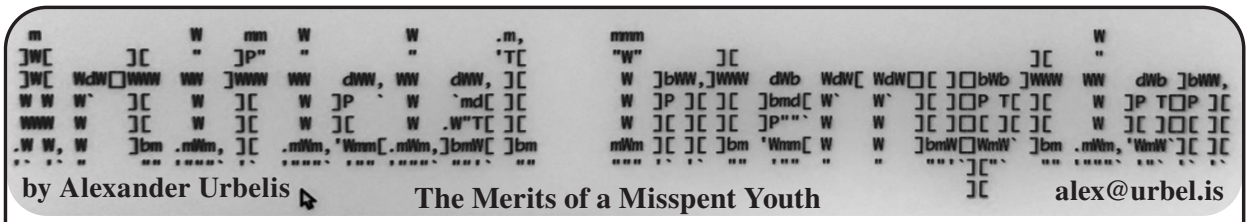
[7] "Don't Sell Your #Bitcoin Unless.. - Michael Saylor" ; User : h0wusayit ; www.youtube.com/watch?v=jK2b0g_6pfY
[8] Beeple : "The First 5000 Days" ; Christie's online auction listing; onlineonly.christies.com/s/beeple-first-5000-days/lots/2020
[9] "Beeple Explains The Absurdity of NFTs | So Expensive", *Business Insider* ; www.youtube.com/watch?v=nTmF26NUZTA
[10] "thoughts on Tom Bilyeu explaining NFTs to Quentin Tarantino?", Executive Wave ; www.youtube.com/watch?v=h0kejs3fuz8
[11] Scrt.Network blog: "Announcement: Announcing the Tarantino Community Drop!"; Nov. 8, 2021; staging.scrt.network/blog/announcing-the-tarantino-community-drop
[12] "Quentin Tarantino's Secret NFTs", *The National Law Review* ; Dec. 8, 2021; www.natlawreview.com/article/quentin-tarantino-s-secret-nfts
[13] "Inside The Fight Over The 'Pulp Fiction' NFT", *Variety* ; Gene Maddaus, Sep. 28, 2022; variety.com/2022/film/news/pulp-fiction-nft-secret-network-guy-zyskind-1235384962/
[14] "How Bitcoin's Peer-to-Peer Cash System Was Revealed 11 Years Ago"; Jamie Redman, Oct. 31, 2019; News.bitcoin.com ; news.bitcoin.com/how-bitcoins-peer-to-peer-cash-system-was-revealed-11-years-ago/
[15] "Explained: How Bitcoin transactions compare to FedWire" ; Protos Staff - Sep. 22, 2022; Protos.com ; protos.com/explained-how-bitcoin-transactions-compare-to-fedwire__trashed/
[16] "The Case For Bitcoin: High Portability"; bitcoin.onelshina.com/high-portability
[17] "Bitcoin Is An Actual Coin: Myth"; *Fact/Myth* ; Thomas DeMichele, May 18, 2018; factmyth.com/factoids/bitcoin-is-an-actual-coin/ . 1st paragraph : "Bitcoin isn't a literal coin; it's a list of transactions recorded on a shared digital public ledger called a 'block chain'. All 'coins' are stored in digital bitcoin 'wallets' and can be verified against the ledger."
[18] "Cryptocurrency Taxes"; Joe Liebkind, July 23, 2022; *Investopedia* ; www.investopedia.com/tech/taxes-and-crypto/
[19] "Biden's cryptocurrency framework is a step in the right direction"; Mitesh Shah, Sep. 28, 2022; *CoinTelegraph* ; cointelegraph.com/news/biden-s-cryptocurrency-framework-is-a-step-in-the-right-direction
[20] "Why Cryptocurrency Regulation Is Actually 'A Good Thing' for Investors, According to These Experts"; Alex Gailey, April 19, 2022; *TIME* ; time.com/nextadvisor/investing/cryptocurrency/why-crypto-regulation-is-good-for-investors/
[21] "Right Click, Save As? NFTs Explained!"; User: keepfischin, Aug. 15, 2021; *Medium* ; medium.com/sidechain/right-click-save-as-nfts-explained-7ee2734aea52
[22] "Anatomy Of an NFT Smart Contract"; User: Crypto Futurist, Jan. 15; *Medium* ; medium.com/geekculture/anatomy-of-an-nft-smart-contract-56a66bc07902
[23] "Anatomy of Smart Contracts"; Last Edit - User: @wackerow, Aug. 15, 2022; Ethereum.org ; ethereum.org/en/developers/docs/smart-contracts/anatomy/
[24] "Introduction to Smart Contracts"; Last Edit - User: @wackerow, Sep. 1, 2022; Ethereum.org ; ethereum.org/en/developers/docs/smart-contracts/
[25] EtherScan.io tutorials: "Tokens"; docs.etherscan.io/api-endpoints/tokens
[26] "How to Build an NFT Marketplace - Solidity Tutorial (for Beginners) [2022]"; User: HUSNAiN, Nov. 29, 2021; www.youtube.com/watch?v=84j71K6wOCs
[27] "Code an NFT Marketplace like OpenSea Step-by-Step [ERC-721, Solidity]"; User: Dapp University, March 11, 2022; www.youtube.com/watch?v=2bjVWclBD_s
[28] "Ethereum Smart Contract Backdoored Using Malicious Constructor"; User: LiveOverflow, March 10, 2019; www.youtube.com/watch?v=WP-EnGhIYEc
[29] "How To Store NFTs On A Hardware Wallet"; Trezor Blog; User: SatoshiLabs, Dec. 20, 2021; blog.trezor.io/how-to-use-nfts-with-a-hardware-wallet-9b4308397ea7
[30] "Running Your Own Bitcoin Node, Ethereum Node, Lightning Network Node - aantonop Q&A"; User: aantonop, Feb. 7, 2021; www.youtube.com/watch?v=AXUfwvhr3lg
[31] *Mastering Ethereum* gitbook by Andreas Antonopolous, "Should I Run A Full Node?" ; github.com/ethereumbook/ethereumbook/blob/develop/03clients.asciidoc#should-i-run-a-full-node
[32] "Celebrities are Running the Biggest NFT Scam Ever"; User: Everything Science, Feb. 22, 2022; www.youtube.com/watch?v=SPXwNm5fjQ4
[33] "Jimmy Fallon Faces LAWSUIT After NFT Scam On Live TV"; User: Viral Vision, Feb. 2, 2022; www.youtube.com/watch?v=FjvXytkuf5I
[34] "Money Transmitter Licensing For U. S. Crypto Companies"; July 13, 2020, Author: Kelman PLLC; Website: Kelman Law; kelman.law/insights/money-transmitter-licensing-for-u-s-crypto-companies/

The Hacker Digest

Every full volume of *The Hacker Digest* has now been digitized into PDF format. Each digest is comprised of that year's issues of *2600*. That means you can now get every single year of *2600* going back to 1984. If you're the kind of person who wants it all, then this may be just what you've been waiting for.

For $260 you can get EVERY YEAR from the beginning and EVERY YEAR into the future (future digests delivered annually) - all completely copyable and able to be viewed on multiple devices. You'll be amazed at how much hacker material will be at your fingertips. (If you already have a lifetime subscription to the magazine, you can add all this for $100.)

Visit *store.2600.com* to subscribe!



by Alexander Urbelis

The Merits of a Misspent Youth

alex@urbel.is

Pittsburgh is a town with an unfortunate name. I recently had the chance to visit for a speaking engagement at the annual conference of the National Cyber-Forensics Training Alliance. Pittsburgh is a lovely city: historical, green, full of bridges, with no fewer than three rivers: the Allegheny, the Monongahela, and, where those two bodies meet, they forge the Ohio River. It was anything but the pits.

Looking into its etymology, I learned that Pittsburgh was named after William Pitt the Elder, Earl of Chatham, the former Prime Minister of Great Britain from 1766 to 1768. Curiously, William Pitt the Elder was also known as the Great Commoner because of his enduring refusal to accept a royal title until 1766. The "burgh" in Pittsburgh was a nod to William's Scottish roots, where the names of towns often ended in "burgh," though the Scots made noises that sounded more like "borough."

Incorporated in 1816, the founding document of Pittsburgh contained a typo - every reference was spelled without the ending "h." For many years, no one could agree whether to spell the town as "Pittsburg" or "Pittsburgh." The train station's portico left out the "h," the federal government never used the "h," but native Pittsburghers insisted on the inclusion of this consonant. It wasn't until nearly a hundred years later, in 1911, that local political forces came together in a bipartisan celebration of consistency, formally returning the missing "h" to Pittsburgh. This absurd bit of history made Pittsburgh an altogether more fascinating place. There was a similarity to my youth, to our youths, spent as hackers, through which our mistakes have made us all the more remarkable and, in many ways, shaped our futures.

I often joke that it was my misspent youth as a hacker that has propelled my career as a lawyer more than anything else. And coincidentally, at the outset of my talk to the NCFTA audience in Pittsburgh, I told a story about this very point. This story seemed unbelievable, one of those anecdotes that is entirely true but, if you saw it on television, would strain your sense of credulity.

The story in question is about how I came to be the CISO of the NFL. (Why I was asked to interview for this role is another story entirely, for another day.) Suffice it to say that it was a humid, early September day in 2019. I was wearing a full suit and tie, and took the F train uptown to the NFL's headquarters on Park Avenue. As the New York-based readership can attest, the subway in the summer can feel akin to what one would imagine a Native American sweat lodge to feel like. Having arrived on the sixth floor of the NFL headquarters, I had to ask to excuse myself so I could use paper towels in the bathroom to blot the copious amounts of sweat running down my forehead, neck, and armpits, etc., before entering the room containing my interviewers.

When I entered the room, recovering from hyperhidrosis and still overheated in all the expected areas, my interviewers were already there: two women and one man. The first woman was (and still is) the current chief security officer of the NFL, and prior to that she was the chief of police for the District of Columbia. The second woman was the head of governance, risk, and compliance. The man was a vice president in the IT department.

Starting with the CSO, I introduced myself and shook hands. The man, an Italian-looking guy on the shorter side with wispy brown hair and a bit of beard, introduced himself as Aaron, gave me a peculiar look and said, "I know you, man."

This was shortly before the pandemic, so my facial hair consisted entirely of my trademark handlebar moustache. A recognizable and memorable feature, self-important me thought that this Aaron character must have recognized my face from, perhaps, a television appearance of mine, one of my CNN Opinion pieces, maybe my articles for *FT*, or something like that.

"That's great," I said in response and thought we would move on. With abnormal persistence, Aaron responded, "No, I *know* you, man." "Ah, OK, I appreciate that." I hoped that would be the end of this awkwardness.

But then I heard something that no one has brought up for a good 20 years or so. Pointing at me, and with the CSO and head of GRC looking curious as to where all this was going, Aaron said, "You're Neon Samurai." "Holy crap," I thought to myself. That was my hacker handle from the mid 1990s! How could this guy know that? I then started thinking about the fact that the NFL has their own intelligence unit, so perhaps it wouldn't be unreasonable to expect a form of undue and over-the-top diligence on those they're thinking of onboarding.

At this point you can't deny it, so I confidently

and without hesitation said, "Yeah, that's me. Now, who the hell are you?" With a smile cracking on his face, Aaron stepped towards me and said, "Do you recognize my face now? I'm Arkane."

Memories flooded back. I immediately recognized him at this point and understood why he was weirdly persistent moments ago: we were hackers together on Long Island in the 1990s, we were great friends, and I hadn't seen him in over 20 years. "I don't believe it," I said. A hug ensued. The CSO and head of GRC were simultaneously confounded and amused. Aaron then said, "Chief, I think the last time I was hanging out with Alex was in his parent's house on Long Island - we were cloning cell phones in his bedroom with an EEPROM reader/writer." "Uhhh, that does sound about right," I responded. To which Aaron said, "I can honestly say, if there's anyone who understands how hackers think, it's Alex."

To abbreviate this longwinded story, the interview started. I was way over-prepared because I don't like to lose. And I wound up becoming the CISO of the NFL.

Because of the shared history and friendship that Aaron and I had as hackers, there was no getting up to speed or sizing up your counterpart. We worked together like old friends. And precisely because of all of the crazy things we had done together in our misspent youths, I had no question that he knew his shit, and he had no question that I knew mine. As readers who work in cybersecurity will know, there can sometimes be friction between the IT and cybersecurity teams. When the heat from that friction started to agitate our respective teams, Aaron and I would have lunch and we always worked out an innovative way to bring down the tension and accomplish our missions. I'm proud to say that Aaron is now the deputy CIO of the NFL and even prouder to say that I count him as one of my dearest friends.

A few months ago, I was at an invite-only Chainalysis VIP dinner associated with their Links conference in New York. Putting aside the questionable location of the dinner - the terribly touristy Times Square - the venue was chock-full of people working in the blockchain forensics space. I sat at a long table with a dear Chainalysis colleague who had invited me to the dinner. Two tables away, I saw something familiar. Between the several bodies obscuring the item, I could see what was clearly a black t-shirt with what appeared to be an electronic schematic in white on its front. You, me, and any longtime reader of this rag would instantly recognize this as a *2600* blue box shirt. I made it my mission to make my way over to this man by the night's end.

Recognizing this, I said to my companion, "That guy is an old school hacker, and he wants people to know it." Going further, I speculated, "My guess is that he's wearing that shirt as a sort of flare - to send a signal to anyone else out in the room that recognizes the shirt." After massive salads and about 30 pounds of pasta was served to our collective tables, I made my way over and tapped this guy on the shoulder. "Excuse me, I couldn't help but notice your blue box shirt." "Thank you!" he shouted over the din of the dinner. "I have been wearing this shirt for the last two days at the conference wondering if anyone would recognize it, and you're the only person who's said a word about it."

My companion was with me when this happened. I remarked to my new *2600* friend that I had said to her that I believed he was wearing the shirt as a message to others that he was an old school hacker. "Exactly, exactly!" he said. This guy and I became instant friends. I will not mention his name, company, or affiliation, but suffice it to say that he does quite stimulating work tracking dark money across blockchains, with a specialization in sub-Saharan Africa, and so has eyes on all sorts of treacherous transactions and perilous persons. We stay in touch and I know that I can call on him for any aid or assistance and he knows that he can call on me for the same.

These bonds and friendships that involve *2600* and the hacker subculture are strong. They're also weird. They can run deep in our veins for three decades, like the friendship between Aaron and me, or be made instantly and indestructibly as was the case with my newfound dark money-tracking friend. This raises the obvious question of "Why so?"

The bonds of a shared experience provide a solid foundation for sure, but the kinship is richer than that. We share an ethos, a value system, and a philosophy, not unlike the Freemasons. We don't have our own secret handshakes, but we do have our own esoteric modes of recognition: when you see another wearing a *2600* shirt, you have found your tribe. We don't meet in the Lodge, but we meet at HOPE and other like-minded conferences. Like the city of Pittsburgh, our historical imperfections are what make us interesting and who we are.

We are not afraid to roll up our sleeves to take apart devices, or to take on systems, and we put the pursuit and sharing of knowledge above all else. We stick together. We must pass this on. And we must ensure that the next generation has the opportunity to make the same mistakes as us, with as much mirth and as much hope, so that they protect and pass on this wonderfully bizarre culture of ours.

A Tale of Insecurity

by JMT

I am not a hacker. I once dumpster dived at a bank, but found only coffee grounds and empty coin wrappers. I wardialed in the 90s, and had an interesting conversation with a man who *69'ed me and accused me of sleeping with his wife. I am sure that if I had met the right person at the right time, things would have gone very differently for me. There is certainly an alternate universe in which I'm in jail for violating the CFAA, and another where I'm a CISO. But in this one, I am just a guy with a strong password and a subscription to *2600*.

In the mid aughts I worked at a law firm. We had an incompetent IT manager who outsourced all the real work of running an office IT department. The one thing he did himself was routinely email all staff demanding that we report our passwords to him. As abhorrent as I found this practice, I enjoyed the ability to pay my rent. So I always dutifully complied, and then promptly changed my password.

One night I was working late and wandered into a conference room where an office-wide desktop refresh project had been underway for a week. Our outside IT consultants had commandeered this room as their base camp, and the large table was covered with Dell OptiPlexes in various stages of being re-imaged and configured for their new users. At 9 pm on a Thursday, the conference room was now deserted, and I was one of only two or three people in the entire office. Reasonably confident of my privacy, I took my time looking around.

I didn't expect to find anything. I wasn't up to no good. I was just looking. Just curious. In time, my eyes landed on a single sheet of paper in the middle of the table. As a paper it was unassuming, but it stood out amongst all the cables and molded plastic. I looked closer, focused, and nearly fell over in shock.

Lying in the middle of the table in an unlocked conference room was a printout listing every employee's name, login, and plaintext password. Everyone. Me, my boss, his boss, their secretaries, the partners. Everyone. In one of the fastest decisions I've ever made in my life, I grabbed it and walked confidently to the nearest copy machine. I made a single untraceable copy (no employee keycode required), returned the original to its dubious home, and went back to my desk to examine my booty.

The average quality of my coworkers' passwords was absurdly low. Simple alphanumeric strings like password1, qwerty, and their children's names protected nearly every account in the firm. One after another, I read down the list and realized that I could have guessed half my coworkers' passwords in less than five minutes, had I ever tried. A proper dictionary attack would have cracked most of the rest instantly.

But the biggest surprise was the strongest password. It didn't belong to the IT manager, or to a young, tech-savvy attorney. It belonged to a 76-year-old founding partner, and I'll never forget it: purplecow.

A dictionary attack would have made short work of this one, too, of course. But you wouldn't guess it. It was only in context that it became impressive - a Dachshund among Chihuahuas. But at least he tried.

That night was exhilarating for entirely juvenile reasons. I had no use for it, but possessing such forbidden knowledge just felt so cool. Had I become 1337? Was I about to be "in?" No, I had no interest in reading my boss's email, finding out what my coworkers really thought of me, or losing my job.

I never did anything with my sudden godlike powers, though I kept that paper for years. I loved having it for its own sake, and I still love telling the story of my greatest near-hacking experience.

Start your own *2600* meeting!

It's easy and fun!

1. Pick a location.
2. Spread the word.
3. Let us know.

Full info can be found at www.2600.com/meetings.

Microsoft, Stop Reading My Emails!

by D33r

On an engagement that simulated access as a typical remote worker, I wrote a very simple custom executable intended to serve solely as a proof-of-concept. The purpose was to test the in-place email security controls and illustrate to the client if a malicious file could be delivered over email and executed on a remote worker's laptop. The payload was written quickly in Python and turned into an executable using PyInstaller without too much interest in the evasion of anti-virus products (though I have seen PyInstaller executables hold their own against some anti-virus products). I also wrote a corresponding multi-threaded Command and Control (C2) server in Python and deployed it on a VPS with a public IP address and tied it to a domain for testing. As things tend to go when hacking computers, events took a strange turn. The email filter wound up doing a little more than expected!

The setup was as follows: we were to send a malicious email from an external user to the simulated employee's MS365 account (we had a physical employee-issued laptop for a more realistic simulation) and would then attempt to click on the attachment. We went through the typical list of executables/malicious attachment files such as .HTA, .HTML, .JS, .EXE, .DLL, etc. to give a well-rounded assessment of their email security filters. Most of these went as expected... besides the .EXE file that was attached!

The email with the EXE was never delivered (unsurprisingly) as described in Microsoft's Outlook documentation that shows blocked attachments (`support.microsoft.com/➥en-us/office/blocked-➥attachments-in-outlook-➥434752e1-02d3-4e90-9124-➥8b81e49a8519`). Suddenly, I noticed that my C2 server had captured a shell from a host! Heart pounding and sweat forming, I thought I had inadvertently done something wrong! Did I send the attachment to the wrong person? Was there a typo in the email address? A slight panic rushed over me as I feared the sounds of federal agents at my door were soon to be heard.

Conveniently, the first stage of the payload was instructed to send host information such as IP addresses, usernames, and the hostname. The payload determined the host was a Windows 10 machine with AMD64 architecture and was executed as the user account "CherryBerry". An effortless ICANN lookup of the origin IP address that was displayed in my C2 server revealed the machine was located at a Microsoft data center. I soon realized that I had not made a mistake, but Microsoft had taken the liberty of executing my code (what an honor!)! "CherryBerry" sounds like something I would name a sandbox account, so I felt assured that this was merely a simulation. Fortunately, I had not just unleashed a plague on the digital world!

Interestingly, the executable was placed in the Outlook directory just as a normal email attachment would be. I suspect this is to prevent sandbox evasion techniques and to simulate an actual user clicking on the email. After executing a few basic commands to verify my theory such as "dir" and "ipconfig", I captured my screenshots to show the client and my colleagues this puzzling event, then promptly closed the shell and terminated the session. After starting to wrap up this section of the engagement, Microsoft continued to execute the malware on many additional sandbox instances. This resulted in a barrage of shells with similarly humorous usernames until I finally stopped my C2 server and destroyed the VPS I had created.

This hilarious and surprising situation highlighted a case study surrounding the everlasting debate between privacy and security. Is this invasion of privacy in user email accounts justified to keep users "safe" in their own inbox? I am relatively certain that deep within the privacy policies of Microsoft, I agreed to this digital surveillance somewhere. Though I certainly did not anticipate them stealing my email in transit and to then execute arbitrary code.

The Cybiko

by 2600 Article Submissions, Jr.

Gather round while I tell a story about an ingenious device born in a time before the Imperial Decree that the whole world must carry an always-on, trackable computer in their pockets, ostensibly since said computer also makes phone calls. Friends, Romans, countrymen, lend me your ears, I come to exhume the Cybiko handheld.

Let's start by taking a look at the hardware itself. The first image that enters your head when you see a Cybiko is that of a pocket calculator designed by Salvador Dalí, endowed with a transparent case rendered in retina-searing colors. That image might make you turn away there and then, but that would be your loss. This freakish artifact is really a treasure trove of useful functionality for the hacker.

The creators of the device might have realized that the vomit-inducing aesthetic of the first generation units wasn't for everybody: its successor, the Cybiko Xtreme, looks more like an early cell phone that was run over by a smallish car. *Chacun à son goût*.

But don't be deceived by the odd looks. When you take a peek under the hood of one of these doohickeys, you will find a rather impressive setup for a handheld of the era:

- A Hitachi H8S 32-bit processor running at 11 MHz
- - An Atmel 8-bit coprocessor running at 4 Mz
- 256 KB RAM
- 512 MB flash EPROM (expandable to 1 MB)
- An RS-232 port
- A parallel bus expansion slot
- A two-way radio for the 900 MHz sub-GHz band
- A plug-in MP3 player
- A gray-scale LCD display 160 x 100
- A full QWERTY keyboard with pencil eraser style buttons

Before you turn up your nose, please consider that this device was born in the year 2000, a time when desktop PCs had barely graduated from 16-bit to 32-bit architectures, and the majority of consumer systems ran Windows 95 or its ugly sister, Windows ME.

The Cybiko Xtreme came out a year later with a faster clock speed of 18 MHz, a mouthwatering 1.5 MB of RAM, and an improved OS. Instead of the good old RS-232 cable, it had one of those newfangled USB ports that all the cool kids wanted.

If the hardware was impressive for the day, the functionality was even more so, if a bit schizophrenic. It was almost as if the creators couldn't decide whether they wanted to build a handheld game console, a calculator, a walkie-talkie, a music player, a PDA, a Tamagotchi, or something else entirely, and finally gave up and put all of that functionality in a single gadget. Here's a condensed list of what it can do:

- Games. You could download hundreds of them for free
- Text messages
- Two-way radio communications
- Email, using a PC's Internet connection
- Text editor
- Calendar
- Multilingual dictionaries
- Scientific calculator
- And much more through software downloads...

If you're with me this far, you're probably hopelessly sold on the idea of owning a Cybiko and desperately want one. You can find usable units with chargers and cables on eBay and Craigslist for a couple of tenners. Be prepared to pay about $100 for a new-in-box unit if you can find one. When you get yours, make sure you swap out the leaky dot-com-bust era batteries for something a little newer. Then download a few games and familiarize yourself with the device. Once you're done with that, we can move on to more serious things, like how the Cybiko fits into the hacker's arsenal.

The first thing I'd like to point to is the RS-232 functionality. I'm sure many readers of this publication can think of interesting things to do with a handheld RS-232 terminal. The fact that the terminal in question looks like a cheap, old children's toy adds to the stealthiness. The end of the serial cable that connects to the Cybiko has a proprietary connector, and replacement cables are hard to find, but there are instructions online on how to work around this. The "business end" of the serial cable is a common-as-dirt DE-9 connector.

Next, let's consider the RF subsystem. The Cybiko can connect to other Cybiko units nearby, kind of like Bluetooth, except it isn't Bluetooth and therefore not easily detected by modern gadgets. The U.S. version of the Cybiko divides the spectrum between 903 MHz and 928 MHz into 30 channels, each capable of supporting 100 devices, making a mesh network of 3,000 devices possible. (Incidentally, this is the same spectrum used by various LoRa frequency-hopping devices.)

The range of the RF subsystem is a mere 300 feet. At first glance, this might seem like a serious limitation, but in many situations it's a boon. Imagine a scenario where you really don't want your communications to be tracked. Cell phones and CB are out of the question, of course, and Bluetooth is far too promiscuous. But what are the odds that somebody with a sub-GHz scanner is within 300 feet of yourself and those you wish to communicate with?

In situations where the distance-limitation becomes an issue, multiple Cybiko units can

easily form a daisy-chained mesh network, as long as adjacent nodes are within range of each other. This can be used not just for human to human communications; other things, such as RS-232 communications and other binary protocols, can be relayed across the links, opening up many possibilities for remote access.

Interestingly, some Cybiko apps could be set up to jump from one device to another. An example of this was a Tamagotchi-like digital critter that could "escape" to another Cybiko if its owner "neglected" it. If harnessed, this functionality could, for example, be used by people living under oppressive regimes to transfer artifacts by close encounter without knowing the other's identity, plausible deniability at its finest. Other uses might come to mind.

The plug-in MP3 player accepts standard MMC or SC cards that can be used for data storage and transfer. There is a 64 MB size limit, probably imposed by the OS.

If the application downloads don't offer what you need, do not despair. There are several SDKs for the Cybiko with which you can develop your own tools and applications. Supported programming languages include a BASIC dialect, C, and C++. Alternative operating systems, boot loaders, and flash images are also available online.

Finally, the expansion slot has the same footprint as a PCMCIA card. Unfortunately, it is not pin-compatible with PCMCIA, but the signal layout is well-documented online. In theory, you could rip the guts out of an old PCMCIA card, solder on some wires, and connect it to just about any piece of hardware imaginable. In practice, you probably want to use a PCMCIA breakout card unless you're a beast at soldering.

Here are some online resources to get you started on your Cybiko journey. Some of the resources contain links leading further down the rabbit hole.

- mirror.jcx.life/cybiko/
- cybiko.net/cybiko-xtreme/
- famicoman.com/2021/06/23/2021-06-23-using-a-cybiko-as-a-serial-terminal/
- news.ycombinator.com/item?id=10079069
- kn100.me/interfacing-with-cybiko-2022/
- www.piclist.com/techref/cybiko/sdk3012/cybiko _ sdk _ 3012/StartDev.html
- bluecybiko.tripod.com/bluecybiko/id14.html
- www.devrs.com/cybiko/
- www.piclist.com/techref/cybiko/c.htm
- www.dbzoo.com/cybiko/unixh8compiler

Turing's Battle

by Michael Wild

The simulation's graphics are elementary. From what Alfred could tell, this was a more table-driven and list game more akin to an Excel spreadsheet than *World of Warships*. But, he was told, it made surprisingly good moves and could be easily programmed with various scenarios from WW2 to the late Cold War and maybe some things from more current. "It," Alfred ruminated, was a new artificial intelligence naval opponent.

The basic structure, he was told, allows working with a cutting-edge AI. The table-based game and its turn structure were made to enable the computer folks to build a perfect opponent. Amazing graphics like *World of Warships* could follow once the AI could win game after game. Alfred is a historian and game player - tabletop, not computer - and had been asked to play against the AI.

Alfred smiled at the names of his ships for this scenario, "Not Midway," all South American heroes and locations. He knows, being a historian, that in the past, the Navy exercise fleets were called Red and Blue, using the names of the existing ships. "But this is a fictional construct, and instead of using any real names and upsetting a government or U.S. naval folks when the inevitable leaks happen, they picked a South American mix," explained one of the designers of the game. A young kid in a dark t-shirt and shorts. Thus, Alfred found he had three aircraft carriers in his fictional fleet: *Rio de Janeiro*, *Benito Juárez*, and *Simón Bolívar* for CV-1, CV-2, and CV-3. All conventionally powered and carrying less aircraft and firepower than a U.S.-styled Nimitz or Ford-class carrier. They seemed to correspond to certain China-built carriers, Alfred observed.

Alfred, running queries, can see the basic breakdown of these ships now reduced to just a few factors. He has many cruiser-sized destroyers, regular destroyers, some missile and other anti-submarine focused. In addition, there is a collection of submarines, some useless pre-Cold War copies of U-boats, some conventional Cold War models, and some surprisingly powerful nuclear submarines, *Argentina* class - likely a copy of Soviet Cold War boats.

The scenario allows him, the aggressor, to pick his target for victory. He is to pick Alaska or Hawaii. Alfred thought, "'Not Midway,' indeed."

His terminal shows a list of his forces: most of his ships were conventionally powered; for the short time that the scenario covers, he was told he did not have to consider the placement of oilers or resupply his warships.

"Let's go alternative history," Alfred says to himself. He creates a task force with fast cruisers and missile destroyers with ship-to-ground weapons, with the conventional carrier *Rio de Janeiro* as the focus. He heads them to a point near Hawaii, where the 1941 attack was launched. "If you are laying bait, it is best to be obvious," Alfred says gleefully to his terminal. "And like any WW2 aggressive plan from 'South America,' I will split my forces," he says to himself, creating another task force and pointing it at the alternative-history selected victory objective, Alaska. He establishes two task forces of submarines as a vanguard for his Hawaii attack. The lesser submarines will arrive before his forces and will likely get noticed. The small quantity of nuclear subs is sent out early and are in silent (and slow) mode when approaching Hawaii to intercept any defenders. He placed them north of Hawaii near the original American position for Midway in 1942. "Should always cover the obvious," he says to himself.

"Now for the real attack," he says. *Benito Juárez* repeats the Midway plan and attacks small targets like Dutch Harbor with planes and some missiles. Seward is a tourist town, but it will get some morale-busting attention. Next, *Simón Bolívar* will take on the air force bases, destroy the Alaska oil pipeline, and prepare for the land invasion of the Anchorage area. "Midway has moved north and is now the Battle for Alaska," Alfred says. "Try that out, AI," he thinks to himself as he sends out his last commands to start his part of the game.

Tim is a soon-to-retire commander in the U.S. Navy. He has been voluntold to support and participate in the new AI program. He has been promoted to virtual flag rank in the scenarios to command fictional U.S. Navy fleets. He is currently playing the "Not Midway" game against an aggressive "South American" AI opponent. Tim is overseeing a substantial virtual force - way above his pay grade, but he thinks, "What the heck, I am retiring soon - let's do this."

He reviews his forces online, and the charts and processes remind him of the old Avalon Hill board game *Midway* he used to play against his dad. The warships and classes of ships have been renamed, and the capabilities are summarized to just a few essential values. His first responsibility for the virtual command is to arrange his forces in response to some basic intelligence. The enemy will likely attack Hawaii and Alaska. He notes that the enemy forces include three conventional carriers that match a particular China carrier. The briefing includes his goal: If the enemy's target should become unprotected, the enemy will win, and the land will be occupied.

"We will not be repeating history today, I see," he says to himself. He arranges his four nuclear aircraft carriers into two task forces with two carriers together in each. The names of his ships are American but not current. *Lexington* is a class of carriers resembling a cold-war version of the Nimitz. He has *Lexington*, *Saratoga*, *Ranger*, and *United States* as his main force, CVA-1 through CVA-4. He has ten destroyers, standard multi-use expensive machines, typical of the current American design for destroyers, here named the *Shark* class with just numbers, DD-1 through DD-10.

"Concentration is the best defense against an aggressive enemy - Lee did not enjoy attacking a reinforced position at Gettysburg," Tim thinks. So he splits all the destroyers between the two task forces. Tim also has some *Wolverine* class nuclear attack submarines - another name not in use - which he is tempted to send on a hunt-and-destroy mission. Instead attaches them defensively to the same task forces - these resembling the *Los Angeles* class Cold War versions. "If you concentrate your forces, then do that," he reminds himself.

Where to deploy is the next question. Tim remembers that the Americans deployed north to have some coverage of Alaska in the original Midway battle. Tim smiles and sends his ship south and around Hawaii. Remembering his father's tricks in the old board game. "Never go where the history books tell you - someone has read that book too," was his father's explanation after a bad moment for the then young Tim playing the Japanese forces in the out-of-print game. "One more time, dad, for old-time's sake," he says out loud as if talking to his father.

Tim, now with a plan, reviews his setup and plans. He set his task force to run quietly and to zigzag. This is not to avoid torpedo attacks like in the World Wars. Instead, he orders the zigzag to prevent his task force's wake from appearing on a satellite, giving away his position, speed, and direction. The order is done by just a setting on his task forces he observes and costs 20 percent of the speed. "Worth it, I think," he says as if talking to his dad.

Alan is the computer scientist or the newly created title *data scientist*, and he is watching the scenario named suggestively "Not Midway."

He has two human players thinking they are playing not a human but a cold-hearted and possibly incompetent artificial intelligence simulation. Alan is calling it a *Reverse Turing.* He remembers that another Alan, Alan Turing, famously imagined a day when a computer's response would be indistinguishable from a human's response; this is called the Turing test. Today, his human players thought the computer was an AI and not a human. Thus, they would make, intentionally or not, assumptions about their opponent. As a result, they would not try to outguess or out bluff a human but instead, try to outplay the computer opponent.

Alan is tracing the players' actions. He has many values he is generating from the game, such as force structure, amount of information available to the players, aggressiveness, and how much information is provided to the players. These will all become parameters in a set of equations that Alan might use a simple regression process to solve. Or he and his colleagues will use machine learning processes to determine the best parameters to approximate intelligence.

"Yes, we are reverse engineering a historian and a U.S. naval officer," he says to his team members, who mostly ignore him and watch their numbers and refine predictive algorithms to reproduce the same results they see from the players. There are hushed conversations as ideas are discussed, quickly coded, and intensely watched. The mostly introverted computer and data scientists are having a blast; there is barely any noise except keyboard clicks.

Alan and his staff are watching as the action begins to heat up.

The American forces discover the limits of the "South American Alliance" submarine picket line. Alfred is shocked by the losses as the enemy's high-quality destroyers and attack submarines simply remove Alfred's old-styled forces. Alfred is also surprised that a game without graphics could produce such an emotional response. The ship losses are harshly listed on the screen, but the death counts, even virtual, are disturbing. Alfred feels like he has failed the folks and repurposes the nuclear attack submarines, currently in the wrong place, to head south on a hunt-and-destroy mission.

Tim was at first suspicious when he received the first messages of the detection of conventional submarines by his listening destroyers and attack submarines. Still, the signals got stronger, and he decided to act, entering commands into his virtual terminal. In the resulting action, he took no losses but, like Alfred, was surprised by the estimated death counts. Not something he was used to seeing; even for an enemy, it was disturbing.

Tim changed his settings for his task forces. "Time to rush and search," he said to his screen.

Next, Alfred launches his attacks on Hawaii. Within a few moments, he was getting damage reports from his attack. The air strike from his carrier and the missiles destroys most of the airpower in Hawaii. The attack cost was a third of his attacking force, but the missiles and the going in 100 percent on the air strike worked. "If you are going, go big," he said. "Also, I am not going for a second round. Time to run away," he whispered to his computer. He orders the task force to cycle the planes to defensive use and to leave.

And that might have worked, but Tim launched his attack the moment he could and let the pilots and technology direct the battle. "Planes on the deck are targets," he says to himself. With all the noise of the enemy's attack on Hawaii, Tim was soon told that his forces had located the "South American" forces. The enemy aircraft carrier had just landed the planes and only rearmed a few planes and got them in the air before the full attack hits. The missile destroyers did stop some of the attacks, but the main target, the carrier, took most of the attack. Some of the destroyers were also taken out. Tim took 15 percent losses.

Alfred was not surprised that the Hawaiian attack was a success and that the main force was destroyed; a message on his terminal said that *Rio de Janeiro* was a sinking wreck. But his other carrier strike force started on Alaska, and he knew that the virtual U.S. forces must rush to Alaska. Alfred learned from messages that all four enemy (Tim's) carriers were in a pair of close-moving groups. Alfred had his quiet submarines headed into action. "That will be interesting," he was thinking. "It's a trap," he says.

Alan is watching the action and collecting information on how the players react. He is building a model of information on how an AI should respond when supplied with certain facts. His human players provided interesting factors for his models. For example, he noticed that the players' aggression changed with information and threat size.

Alan was trying to discover parameters and turn them into a single value. Like chess programs, he thought to himself, you can measure the King's position and give better values for being moved away from the center - it

is a simple but effective measure. The opposite for major pieces - queen, bishop, and rook - which are more effective towards the center. For a basic chess program, you can just use these calculated values to evaluate legal moves and play basic chess. Likewise, Alan could already see that if he could quantify a value for information and threat size, he could create an equation of aggression.

Alan is already writing a bit of Python code to crunch the data into some linear regression, and even a machine learning model using the random forest of trees approach to see if he can predict the moves that have already happened. Other computer scientists and data scientists are heads down and happy. There is good data coming in!

Tim is not surprised when the *United States* is torpedoed at full speed and then hit with missiles when stopped. A quiet nuclear attack submarine, obviously of Soviet design, has slipped by and killed the carrier. A U.S. carrier is hard to sink, even a virtual one - Tim thinks and smiles grimly. The *United States* is now running at 20 percent. The AI bushwhacked him.

Alan and his fellow scientists watch for how Tim and Alfred react.

Alfred yells, "Yes!" and fist pumps when he sees that the U.S. AI has lost a carrier. Not a flaming wreck, but put out of action. Alfred makes no changes, "Let her ride," he says to himself.

Tim splits his groups apart as they rush to Alaska to stop the incoming invasion. He leaves two destroyers to protect and help the *United States* back to port as he remembers that the game counts causalities. Tim recalls that in World War One the British lost two ships when the U-Boat torpedoed the rescue ships. He is hoping the AI is not going for the WW1 model.

Tim's remaining destroyers are in full ASW mode, and many enemy submarines are now falling to their attacks. No more attacks reach his three remaining carriers, but the fight has slowed his advance to Alaska.

The attack on Alaska is not enough for Alfred to win - he dearly misses the third carrier now. He must risk a more decisive attack and moves both virtual carriers closer to the Anchorage area. Another attack will destroy the remaining opposition and temporarily destroy the oil capabilities of the area. He needs to finish this before the AI stops fighting down south and decides to head north.

Tim shouts, "Damn the torpedoes," and virtually throws his forces into a mad rush north. As soon as he reaches maximum range minus his continued steaming speed, he launches another blind attack into the north. Moments later, the *Saratoga*, like her WW2 namesake, seems to attract torpedo attacks, but U.S. carriers can have a lot of holes in them, and she keeps going with two less important hits. Even in a rush, Tim slows the task forces by 10 percent to match *Saratoga's* reduced speed. This change also allows for more ASW work, and his display shows multiple losses to the enemy soon.

Tim blindly launched an attack, relying on the same tactic as before; this time, it was less effective, and only some of his forces found the enemy. The attack hits one carrier, *Benito Juárez*, which is heavily damaged.

Alfred cannot win. While he withdraws, Alfred's virtual forces fight off some missile attacks. Alfred could get the planes off the *Benito Juárez* and onto the *Simón Bolívar* using his undamaged carrier and thus can assign all his aircraft to a defensive role. He is making a fighting retreat but knows the invasion is off. Alfred will try to exit with as much of his forces as possible. "Next time, we will get ya," he says in his best Captain Ahab accent.

A lucky hit on *Lexington* and again on *Saratoga* reduces the final punch, and Alfred's forces can limp away with both conventional carriers. Tim saves Anchorage from the invasion. The simulation ends.

Alan and all the other scientists are quiet and busy crunching the numbers. They will soon have equations and data models to test against the collected data. They can then remodel the same play and replay the actions of each human player.

Epilogue

Alan was happy that Tim and Alfred would be joining them again. This time it will be "Not Coral Sea," and each player will have an AI advisor and virtual fleet. The initial equations and machine learning models are ready to advise each player. The U.S. player will have an advisor, *Layton*, and the South American player will have one named *Nelson*. Again, Alfred and Tim would think they are playing an AI, which would be partially true this time. Alan and his crew were looking forward to more data.

Alan knows it will take a while, but the final goal is a predictive engine that can provide input into the decisions of a U.S. Naval commander so good that you can't tell it is not human. Turing goes to war in a new age.

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally don't cost a fortune and are open to everyone. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.**

Please remember that we need sufficient lead time (a minimum of three months) to list events in the magazine. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community. All events are subject to change.

August 2-9
BornHack 2023
Funen, Denmark
bornhack.dk

August 4-5
Vintage Computer Festival West
The Computer History Museum
Mountain View, California
vcfed.org

August 10-13
DEF CON 31
Caesars Forum, Harrah's, Linq, Flamingo
Las Vegas, Nevada
www.defcon.org

August 15-19
Chaos Communication Camp
Ziegeleipark Mildenberg
Zehdenick, Germany
events.ccc.de

August 25-27
Blue Team Con 2023
Fairmont Chicago
Chicago, Illinois
blueteamcon.com

September 8-10
Balkan Computer Congress
Congress Centre
Novi Sad, Serbia
2k23.balccon.org

September 9-10
Vintage Computer Festival Midwest 18
Waterford Banquet & Conference Center
Elmhurst, Illinois
vcfmw.org

September 28-29
GrrCON
DeVos Place
Grand Rapids, Michigan
grrcon.com

September 28-30
Texas Cyber Summit
JW Marriott
Austin, Texas
texascyber.com

October 6-8
Maker Faire Coney Island
Brooklyn, New York
coneyisland.makerfaire.com

October 20-21
SecureWV 14
Charleston Coliseum and Convention Center
Charleston, West Virginia
www.securewv.org

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

Marketplace

For Sale

SECPOINT PORTABLE PENETRATOR SOFTWARE. WPA WPA2 WPS WiFi Pen Testing. Vulnerability Scanning & Assessment. Multi User Support. Customize reports with logo, name & watermark. Reports in PDF, HTML format & 19+ languages supported. 26% off Coupon code: 2600 https://shop.secpoint.com/

GUIDEBOOK TO COMPUTER AND SMARTPHONE SECURITY by Brandon of Lipani Technologies LLC has been released. This new security book can be purchased at https://leanpub.com/techgeek. Brandon is a certified CompTIA Security+ professional helping users and companies secure their computers, networks, and smartphones across the country. He says, "The purpose of this book is to educate and teach computer and smartphone users about safety and security online."

SECUREMAC.COM is offering popular anti-malware app MacScan 3 to help protect Mac users from malware, spyware, and ransomware. Download a 30-day trial directly from SecureMac.com. Looking for a new podcast? Check out *The Checklist* by SecureMac on iTunes, Pandora, and Spotify.

HACKERBOXES is your monthly subscription box for hardware hacking, DIY electronics, cybersecurity, and hacker culture. Each monthly HackerBox includes a carefully curated collection of projects, components, modules, tools, supplies, and exclusive items. A HackerBox subscription is like having a hacker convention in your mailbox every month. Free online educational material, free domestic shipping, cancel anytime. Visit us at www.HackerBoxes.com for workshops, boxes, merch, and more.

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From RF Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Now including Offensive Security and Kali Linux branded merch! Check us out at https://HackerWarehouse.com.

Rentals

ATTENTION COMPUTER HACKERS, phone phreakers, and tech-savvy individuals! Are you in need of a digital detox? Check out my house in Bryson City, NC. Nestled in the heart of the Great Smoky Mountains, our home offers the perfect escape from technology. While we do offer Wi-Fi for those who need to stay connected, our cozy cabin is designed to help you disconnect and unwind. Whether you're looking to enjoy the natural beauty of the mountains or explore the charming town of Bryson City, our vacation rental is the perfect home base. And with easy access to hiking trails, fishing spots, and local attractions, you'll have plenty to keep you entertained during your stay. On a clear night, you can see the International Space Station overhead as it orbits the Earth from the hot tub. Also, my wife and I aren't bougie and own a vacation rental because we want to. We do it because we like that house and the area. We moved there in 2017. My wife received an offer to get a doctorate in STEM education from NCSU and we had to take it. Now we offer our home to people who want to stay there for a bit. So why wait? Check the link below to learn more and reserve your spot in our little slice of paradise: shorturl.at/kPQR0

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Your feedback on the program is always welcome at oth@2600.com. New for the pandemic: *Off The Hook Overtime,* Wednesdays at 8:00 pm ET on youtube.com/channel2600. Call in at +1 802 321 HACK!

HACKER CULTURE: A TO Z by Kim Crawley will be published in Fall 2023 through O'Reilly Media. It's a fun mini-encyclopedia covering over 300 topics - from notable hackers to tech companies, from hacker ideals to popular technologies. The book is also full of pop culture references and nerd humor. The book contains original quotes from Emmanuel Goldstein and some fun Easter Eggs. Follow news about the book through @kim_crawley on Twitter or @crowgirl@hachyderm.io on Mastodon.

THE THREAT ACTOR'S DIARY is an edgy cybersecurity blog and hacker resource site that's by hacktivists, for hacktivists with a podcast on the way. We're also the official Dallas Million Mask March info hub. Swing by and subscribe! Created by GhostExodus, founder of the Electronik Tribulation Army. We accept interviews & article submissions! https://www.GhostExodus.org contact@ghostexodus.org <Ghost.exodus.freelance@gmail.com>

COVERTACTIONS.COM is the most comprehensive directory of encryption products anywhere. Search by type, hardware/software, country, open source, platform, and more. Now over 1036 products listed which include 221 VPN's, 192 messaging and 117 file encryption apps. These are just a few of the 28 categories available. There is no faster and easier way to find the encryption product that meets your requirements. Suggestions and feedback welcome. Now featuring news on important encryption issues.

DOC8643.COM: technical details of aircraft from International Civil Aviation Organization (ICAO) Doc8643. This is an educational and reference tool. Check it out at https://doc8643.com.

LEAGUE OF EXTRAORDINARY BUDDHIST HACKERS: Calling Buddhist Hackers, Phreaks, Makers, Preppers, Stitchers, Devs, Medics, Biohackers, Graphics Peeps, Videographers, Kind people, any or all of the above, etc. (Actually the last one is mandatory!) I am looking to build a global crew of persons (Kalyana Mitra) male/female/other (I will even consider aliens from other world systems at this point) who identify with the above description. Please only make contact if you have taken the 3 refuges and you are making some efforts to keep 5 precepts (and 8 precepts on Poya Days etc.) + have some sort of attempt at a daily practice - well at least some days! If you are at that sort of level, please contact me ASAP. Also Buddhist Monks/Nuns, I would love to hear from you, but again please only get in touch if you are keeping good vinaya/precepts. Having said that, I think it would be great to hear from Sangha! In fact, I think perhaps it would be best if one of you (Sangha) were running the outfit? Hack the Planet! Hack Samsara! I believe I have found the ultimate hack... TN8FP - but it requires a team effort, no? .,\/(^_^) & <3 from Blebz (open nick) email: blebz@lxbh.org for more info...

DON'T JUST CELEBRATE TECHNOLOGY, question its broad-reaching effects. 78 Reasonable Questions to Ask About Any Technology - tinyurl.com/questiontech

THE MODERN TECHNOLOGY PODCAST NETWORK contains a growing selection of original audio programming by familiar voices from the hacker world and elsewhere. Our comedies, documentaries, audiobooks, cultural discussions, and more are totally free, completely independent, hacker-produced, CC-licensed, and utterly devoid of commercials. Feed your ears at https://modern.technology

VAGUEBOOKING is a podcast about life lived online,

and our new series "The People's History of the Internet" covers the history of the early Internet and the hackers who shaped it. Tune in for conversations with Phil Lapsley, Lucky225, Rob T Firefly, and many more! Found wherever you get your podcasts and at vaguebooking.net.

Services

CALL INTO THE PHONE LOSERS OF AMERICA'S telephone network interface and hack into our collection of answering machines from the 80s, 90s, and 2000s. Listen to episodes of Joybubble's "Stories and Stuff," old telephone recordings, adventure choosing games, and more! Dial 505-608-6123 or 845-470-0336.

HAVE YOU SEEN THE *2600* STORE? All kinds of hacker clothing, back issues, and HOPE stuff! We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. It's great for giving out presents with a hacker theme - or gift cards are available for those who'd rather make their own choices. The store is constantly getting bigger and more interesting. Please come pay us a visit! store.2600.com or 2600.store

DIGITAL FORENSICS EXPERTS FOR CRIMINAL AND CIVIL CASES! Sensei's digital forensic examiners hold prestigious certifications including the CISSP, CCE, CEH, CCO, and EnCE. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, theft of proprietary data, data breaches, interception of electronic communications, rape, murder, wire fraud, espionage, cyber harassment, terrorism, and divorce matters. We can preserve, analyze, and recover data from many sources, including computers, external media, smartphones, and social media. Sensei Enterprises believes in the Constitutional right to a zealous defense and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's principals have written 18 books on IT, cybersecurity, and digital forensics published by the American Bar Association. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

DOUBLEHOP.ME VPN is actively searching for an acquisition partner that shares our vision (https://bit.ly/3a1bCuM). We're an edgy VPN startup aiming to rock the boat with double VPN hops and encrypted multi-datacenter interconnects. We enable clients to VPN to country A, and exit country B. Increase your privacy with multiple legal jurisdictions and leave your traditional VPN behind! We don't keep logs, so there's no way for us to cooperate with LEOs, even if we felt compelled to. We accept Bitcoin! Use promo code COSBYSWEATER2600 for 50 percent off. https://www.doublehop.me

AFFORDABLE WEB HOSTING & SERVERS: NodeSpace Hosting offers affordable web hosting, email, domains, SSL certificates, and bare metal servers at affordable prices. We are specialists in Proxmox VE hosting and using standard networking - no MAC address filtering on our networks! Check out our hosting at nodespace.com.

ANTIQUE COMPUTERS. From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. http://www.vintagecomputer.net

SUSPECTED OR ACCUSED OF INTERNET-RELATED CRIMES? Stand up for your rights! Be calm, cool, and collected: "I respectfully invoke all of my Constitutional rights, officer. I do not consent to any search or seizure, I choose to remain silent, and I want to talk to a lawyer who represents me." Remember basic game theory and the Prisoner's Dilemma: nobody talks, everybody walks. This is a public service brought to you by freedom defense attorney and *2600* subscriber Omar Figueroa. https://www.omarfigueroa.com/2600-know-your-rights/

KB6NU's "NO NONSENSE" AMATEUR RADIO LICENSE STUDY GUIDES make it easy to get your Technician Class license or upgrade to General Class or Extra Class. They clearly and succinctly explain the concepts, while at the same time, give you the answers to all of the questions on the test. The PDF version is FREE, but there is a small charge for other versions. All of the e-book versions are available from kb6nu.com/study-guides. Paperback versions are available from Amazon. Email cwgeek@kb6nu.com for more information.

UNIX SHELL ACCOUNTS WITH MORE VHOSTS. If you like funny, relevant vhosts for IRC, get a JEAH shell. Also, use our vhost domains for email. Access new and classic *nix programs, compilers, and languages. JEAH.NET hosts bouncers, bots, IRCD, and websites. *2600* readers get free setup. BTW: Domains from FYNE.COM come with free DNS hosting and WHOIS privacy for $5.

DISCOUNT WEB HOSTING AND FREE WEB TRAINING. Squidix Web Hosting provides FREE WordPress training in Arlington, VA for Squidix customers. We provide fantastic web hosting for 1,000s of clients. We love our clients and they love us. Our ongoing *2600* promotion will give you 50% off any hosting service for the first year. This offer valid for any new accounts and includes a free CPanel transfer of one existing website. Sign up at www.squidix.com and use code 2600 on checkout.

LOCKPICKING101.COM is open to hackers wanting to learn physical security and the insides and out of locks and lock picking. Register to join one of the oldest Locksport communities online.

DO YOU HAVE A LEAK OR A TIP that you want to share with *2600* securely? Now you can! *2600* is using SecureDrop for the submission of sensitive material - while preserving your anonymity. Anonymous tips and documentation are where many important news stories begin. With the SecureDrop system, your identity is kept secret from us, but we are able to communicate with you if you choose. It's simple to use: connect to our special .onion address using the Tor browser (2600.securedrop.tor.onion), attach any documents you want us to see, and hit "Submit Documents"! You can either walk away at that point or check back for a response using a special identification string that only you will see. For all the specifics, visit https://www.2600.com/securedrop (you can see this page from any browser). For more details on SecureDrop itself, visit https://securedrop.org. (SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.)

Personals

I'M GATHERING DATA FOR A STUDY regarding the use of technology in United States prisons. For instance, Code 7370 is a web development course. What is the curriculum, how many men have completed the courses, is there data on post-release outcomes? Wisconsin permits prisoners to use Clearbooks for doing tech college work in-cell. I want policies, experiences, how rules are being applied, restrictions, staff comments. I want objective, referenceable sources, things your admin staff have put in writing. I invite prison admins to send me information too. Jason R. Glascock, 3600 Cty Rd D, Janesville, WI 53548.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. If you're an electronic subscriber, please send us a copy of your subscription receipt. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to marketplace@2600.com.

Deadline for Autumn issue: 8/20/23.

2600 DIGITAL SUBSCRIPTIONS

We are putting the finishing touches on our new digital subscription service that will work on PDF and EPUB3 formats. This new subscriber option will feature:

- Minimal subscriber info
- No DRM
- A simple but secure system

Check store.2600.com to subscribe to digital delivery – subscriptions will open this summer.

PLEASE HELP US SPREAD THE WORD

HOPE LIVES ON!

Get The Most Recent Flash Drive From A New HOPE!

That's right, we have every talk that was given at last summer's "A New HOPE" conference on a single 256gb flash drive!

Each talk is available as a video or audio file and can be copied to any device of your choosing or shared with as many people as you wish.

This was our first conference at our new location at St. John's University in Queens, New York City. You can experience or recapture the excitement that was in the air for all three days. A full lineup of talks can be found at xiv.hope.net.

There's an easy-to-navigate digital guide to all of the talks and - while supplies last - you'll also get a printed program and "A New HOPE" badge!

Just $89 (plus shipping) for a gigantic reusable drive crammed full of talks from "A New HOPE." Full details at store.2600.com or write to *2600*, PO Box 752, Middle Island, NY 11953 USA.

"Just as a well-tempered mind guides a virtuous man, a judicious hand must guide the development of artificial intelligence, lest it becomes a perilous tool of destruction."
- what Benjamin Franklin would have said about artificial intelligence according to ChatGPT

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
typ0

Cover
Dabu Ch'wald

Office Manager
Tampruf

STAFF

Infrastructure
flyko

Network Operations
phiber, olssy

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Facebook Team
astrutt, Cryovato, Tina Rose, TechnoMage, danixdefcon5, ItsTehPope, LadyNikon, Osiris

Inspirational Music: De La Soul, Tom Caruana, Dust Raps the Blues, Front Line Assembly, Loreen, Lys Assia
Shout Outs: André the Giant, Big Chungus, Justin Jones, Gloria Johnson, Justin Pearson, Jim & Marilyn Simons
R.I.P.: Aloria

***2600* is written by members of the global hacker community.**
You can be a part of this by sending your submissions to articles@2600.com or the postal address below.

2600 *(ISSN 0749-3851, USPS # 003-176) is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600,*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $31 individual,
$60 corporate (U.S. Funds)
Overseas - $44 individual, $75 corporate

BACK ISSUES:
Individual issues for 1988-2022
are $7.25 each when available.
Shipping added to overseas orders.
All back issues (1984-2022) available
digitally as annual digests at store.2600.com

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

Copyright © 2023; 2600 Enterprises Inc.

MEETINGS

_2600_ MEETINGS CONTINUE TO EXPAND. PLEASE FOLLOW LOCAL HEALTH ORDINANCES IF WARRANTED. KEEP CHECKING THE WEBSITE BELOW FOR MORE UPDATED LISTINGS AS WELL AS INFO ON HOW TO START YOUR OWN MEETING!

ARGENTINA

Buenos Aire: Bodegón Bellagamba, Armenia 1242. 1st table to the left of the front door.
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499. 7 pm

CANADA

Alberta

Calgary: Food court of the Eau Claire Market. 6 pm

FRANCE

Paris: Place de la République, 1st floor of the Burger King, 10th arrondissement.

IRELAND

Dublin: The Molly Malone Statue on Suffolk St. 7 pm

JAPAN

Tokyo: Beemars, Kabukicho, 2 Chome-27-12 Shinjuku Lee Building #2 3rd floor. 7 pm

PORTUGAL

Lisbon: Amoreiras Shopping Center, food court next to Portugalia. 7 pm

RUSSIA

Petrozavodsk: Good Place, pr. Pervomayskiy, 2. 7 pm

SPAIN

Madrid: Maldito Querer, C. de Argumosa, 5. 7 pm

SWEDEN

Malmo (@2600Malmo): FooCafé, Carlsgatan 12A.
Stockholm (@2600Stockholm): Urban Deli, Sveavägen 44.

UNITED KINGDOM

England

Bournemouth (bournemouth2600): The Goat and Tricycle, 27-29 W Hill Rd. 6:30 pm
Cheltenham (@2600Cheltenham): The Bayshill Inn. 6:30 pm
London (@London_2600): Angel Pub, 61 St Giles High St, outdoors at the red telephone box. 6 pm

Scotland

Glasgow (@Glasgow2600): Bon Accord, North St. 6 pm

UNITED STATES

Arizona

Phoenix (Tempe) (@PHX2600): Hurts Donut. 2161 E University Dr. 6 pm
Prescott: Merchant Coffee, 218 N Granite St.

Arkansas

Fort Smith: Fort Smith Coffee Company, 70 S 7th St. 7 pm

California

Los Angeles @LA2600): Union Station inside the main entrance by Alameda St near Traxx Bar. 6 pm
San Francisco: 4 Embarcadero Center, ground level by info kiosk. 6 pm
San Jose: Outside the MLK Library, 6 pm

Colorado

Denver (@denver2600): Denver Pavilions. 6 pm
Fort Collins: Starbucks, 4218 College Ave. 7 pm

Connecticut

Farmington: Barnes and Noble cafe area, 1599 South East Rd.

Florida

Boca Raton: Barnes and Noble on Glades Rd.
Jacksonville (#Jax2600): The Silver Cow, 929 Edgewood Ave S.
Titusville: Krystal, 2914 S Washington Ave. 6 pm

Illinois

Urbana: Broadway Food Hall. 6 pm

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall. 6 pm

Maine

Bangor (Hermon) (@2600Bangor): Bangor Makerspace, 34 Freedom Pkwy

Massachusetts

Boston (Cambridge) (@2600boston): The Garage, Harvard Square, food court area. 7 pm
Hyannis: Nifty Nate's, 246 North St.

Michigan

Lansing: The Fledge, 1300 Eureka St. 6 pm

Minnesota

Bloomington: Mall of America, north food court by Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hackerspace, 2215 Scott Ave.

New Hampshire

Milford: Grill 603, 168 Elm St. 6:30 pm

New Jersey

Somerville: Bliss Coffee Lounge, 14 E Main St.

New York

Albany: Starbucks, Stuyvesant Plaza, 1475 Western Ave. 6 pm
New York (@NYC2600): Citigroup Center, 53rd St and Lexington Ave, food court.
Rochester (@roc2600): Global Cybersecurity Institute, 78 Rochester Institute of Technology. 7 pm

North Carolina

Raleigh (@rtp2600): Transfer Co. Food Hall, 500 E Davie St. 7 pm

Oklahoma

Oklahoma City: Big Truck Tacos, 530 NW 23rd St.

Oregon

Portland: Sizzle Pie Central Eastside, 624 E Burnside St. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St.
Philadelphia (@philly2600): 30th St Station, food court outside Taco Bell (odd months); Iffy Books, 319 N 11 St #2I (even months). 6 pm

Texas

Austin (@atx2600): Central Market mezzanine level, 4001 N Lamar Blvd. 7 pm
Dallas: The Wild Turkey, 2470 Walnut Hill Ln #5627.
Houston (@houston2600): Agora Coffee House, 1712 Westheimer Rd. 6 pm
San Antonio: PH3AR/Geekdom, 110 E Houston St. 6 pm

Utah

Salt Lake City: 801labs Hackerspace 353 E 200 S, Suite #B. 6 pm

Virginia

Arlington: Three Whistles, 2719 Wilson Blvd.

Washington

Seattle: Merchant Saloon in Pioneer Square. 6 pm
Spokane: Starbucks near Wellesley and Division (across from North Town Mall).

URUGUAY

Montevideo: MAM Mercado Agricola de Montevideo, José L Terra 2220, Choperia Mastra. 7 pm

All meetings take place on the first Friday of the month. Unless otherwise noted, _2600_ meetings begin at 5 pm local time. Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle or hashtag so we can stay in touch and share them here! To start a meeting in your city, DM us or send email to meetings@2600.com.

www.2600.com/meetings

Interesting Payphones

Mexico. This is a particularly vibrant looking phone in the midst of a busy street in the sunny surf town of Sayulita. Sure, it's covered in graffiti, but it looks to be in decent condition

Photo by taylorbohn17

United States. Found in Portland, this phone has been set up for free use and reportedly "sounds like an old payphone when dialing." (More on Futel can be found on pages 13 and 47 of 40:1.)

Photo by Creative Resistance

Ukraine. As seen in Lviv earlier this year, this phone takes cards and apparently is still in good working order. It certainly looks like it's seen a lot.

Photo by John Costa

Canada. Spotted in Dawson City in the Yukon Territory, the phone that looks like a permanent part of this building takes both cards and coins and has a dial tone. The fiber assets in this part of the country are now owned by 13 Yukon First Nation development corporations.

Photo by gbn

Visit **www.2600.com/payphones** to see our foreign payphone photos!
(or turn to the inside front cover to see more right now)

The Back Cover Photos

This is Sonia who is apparently as avid a reader of our pages as anyone else. Thanks to **Veronica** for capturing this priceless moment. We open our pages for documentation of any other such interactions with the animal kingdom.

We can only wonder what people passing by on the freeway must have thought as this massive error message was proudly displayed at the Oakland "Oracle" Arena where the Golden State Warriors played basketball until recent years. Witnessed by **Halie Symmons**, this is likely one of the world's biggest shells.

If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues)
and a *2600* t-shirt of your choice.