

EPISODE 757

[INTRODUCTION]

[0:00:00.3] JM: Social media has transformed our lives. It has also transformed how wars are fought. P.W. Singer's new book *LikeWar: The Weaponization of Social Media* describes the far-reaching impact of social media on the tactics and strategies used by military, business and everyday citizens. We've all read stories about Russian bots in Cambridge Analytica, *LikeWar* covers many more cases that are surprising and mildly frightening, from the Gaza Strip to the streets of Chicago to Taylor Swift's Instagram feed, *LikeWar* describes just how pervasive the effect of social media has been on warfare. *LikeWar* also provides historical context.

For software engineers, the repurposing of social media as a weapon is disconcerting. Many of us are working on products with a social networking component. Does this make us complicit in building weapons? We can find some reassurance in the fact that this has happened before. From the newspaper to the television, every new communication invention has been repurposed for war. In a war, a new piece of technology always presents a new vector to gain an advantage in a conflict. Because the stakes are so high in a war, there is a large incentive to find creative ways to use technology to undermine your adversaries and to help your allies.

P.W. Singer has written about robotics, cyber security and modern warfare for a decade. In a previous episode, P.W. Singer and I discussed subjects like Stuxnet, drones and social media manipulation. In today's show, P.W. returns to talk about his book *LikeWar: The Weaponization of Social Media*.

To find all 900 of our old episodes, you can check out the Software Engineering Daily app in the iOS or Android app stores. We have past episodes about digital warfare, national security and other philosophical and pertinent topics. You can check out this app in the iOS or Android app stores and whether or not you're a software engineer, we have lots of content about technology and business and culture and all kinds of subjects that might be interesting to you.

In our app, you can become a paid subscriber, you can get ad free episodes, but you don't have to pay. You can just interact with other members of the Software Engineering Daily community,

you can find episodes that are particularly appealing to you. It's an app that's custom-built for the Software Engineering Daily listenership. I hope you enjoy this episode and let's get on with it.

[SPONSOR MESSAGE]

[0:02:54.8] JM: Triplebyte fast-tracks your path to a great new career. Take the Triplebyte quiz and interview and then skip straight to final interview opportunities with over 450 top tech companies, such as Dropbox, Asana and Reddit.

After you're in the Triplebyte system, you stay there saving you tons of time and energy. We ran an experiment earlier this year and Software Engineering Daily listeners who have taken the test are three times more likely to be in their top bracket of quiz scores. Take the quiz yourself any time, even just for fun at triplebyte.com/sedaily. It's free for engineers. As you make it through the process, Triplebyte will even cover the cost of your flights and hotels for final interviews at the hiring companies. That's pretty sweet.

Triplebyte helps engineers identify high-growth opportunities, get a foot in the door and negotiate multiple offers. I recommend checking out triplebyte.com/sedaily, because going through the hiring process is really painful and really time-consuming. Triplebyte saves you a lot of time. I'm a big fan of what they're doing over there and they're also doing a lot of research. You can check out the Triplebyte blog. You can check out some of the episodes we've done with Triplebyte founders.

It's just a fascinating company and I think they're doing something that's really useful to engineers. Check out Triplebyte, that's [T-R-I-P-L-E-B-Y-T-E.com/sedaily](https://triplebyte.com/sedaily). Triplebyte, byte as in 8 bytes. Thanks to Triplebyte and check it out.

[INTERVIEW]

[0:04:44.0] JM: P.W. Singer, welcome back to Software Engineering Daily.

[0:04:46.4] PWS: Thanks for having me on.

[0:04:47.5] JM: Our last conversation was almost exactly a year ago. In that episode, we talked about some of the contents of your previous books. These were topics like cyber warfare, drones, Stuxnet and some about social media manipulation. Your new book LikeWar focuses completely on the weaponization of social media. Why did you focus on this specific topic for an entire book?

[0:05:13.1] PWS: Gosh. It's a project that our team had been working on for almost five years. Essentially, we were struck by the way that social media was reshaping how we thought about everything from news to politics to war. Then in turn, what was playing out in news, politics and war was reshaping the internet for the rest of us.

What LikeWar is about is essentially that we've seen and grown comfortable with the idea of hacking of networks, the cyber security side of things. That we're now seeing something definitely as important and in some situations, more important the hacking of people on social networks, the idea of driving ideas viral through some mix of our own clicks and likes, but also lies and the network's own algorithms.

It's affected everything from the outcome of elections, to the outcome of what products you buy, what movies you go to. As we explore in the book, it's also affected everything from crime to physical battles; actual wars and the like. We're really struck by it. It's also a world that is filled with all sorts of fascinating characters. Maybe the last thing that really drove us, so it's this mix of it's important, it's fascinating, but that we also felt people weren't getting it. By weren't getting it, what I'm talking about here is this is a space about networking and yet, we were really stove-piped in how we were approaching it.

When I say we, that's everything from the journalists that write on it, the people that work in these fields and the like. For example, the folks that were looking at Isis in the Middle East weren't familiar with what was going on in Russian influence operations in Ukraine. In turn, the people that covered American elections and domestic politics weren't familiar with Russian influence operations, to the people studying criminal behavior weren't familiar with what might be going on in Silicon Valley and how decisions made in boardrooms were shaping the outcomes of what happened in Chicago Street gangs.

The other part of the disconnect was you had some people approaching this field in a quantitative manner, big data surveys of mapping out networks of activities. Then you had other people who were looking at history, or psychology. They weren't bringing their quantitative and qualitative side together. We felt by drawing all this together, we could help unlock some of the secrets of what was going on.

[0:07:54.0] JM: You did draw many different anecdotes together and paired that with your perspectives on those anecdotes. Most people are aware of some of these things. At least in the United States, people talk about what the social media systems have done to our electorate, or to Myanmar, or the Philippines. Your book touches on several other anecdotes that are more removed from at least the western public eye. Can you give a few examples of the lesser-known ways, or the lesser talked about ways that social media is being used to affect a real-world conflict?

[0:08:34.9] PWS: Oh, gosh. It's almost like you're asking for examples. I joke, like asking for which is your least favorite child. I think, let me pull back on it. Maybe a way of answering is one of the things that I've been struck by in terms of the conversations around the book and also just how we talk about social media right now is that we've gone from this period of euphoria and techno optimism where the social media not just could do no wrong, but it was going to fix all the world's ills. If you think about the high point of that was the Arab Spring and the protests that social media played a key, sparking and coordinating role, pro-democracy, pro human rights, the companies Lehman, pun intended into that, and taking credit for all these things that are going on.

Then now we're at the other end of the spectrum, where it just feels so dismal and all the scary effects of this, they were also seeing as you mentioned a couple, whether it's how foreign governments were able to influence domestic politics in a manner that's the scale of it I think is much bigger than most people realize. For example, over 146 million Americans saw Russian propaganda on their Facebook feeds, roughly half the population; most of them still not realizing that.

To the example of Myanmar, genocide essentially coordinated and pushed online. We've had this back and forth. I think one of the things, this is my circuitous way of getting to your question is that you need to understand that there is always going to be both a good and a bad side to any technology, be it the very first stone that was picked up, to social media.

For me, it was the way we tried to show that twin side through characters that showed the duality of it. One of the messages of the book is how social media has been empowering to unexpected players all around the world. We have three little girls in three different locations that I think illustrate that. One of the stories is a heartwarming story of a little girl in Pennsylvania, who at the age of seven starts her own online newspaper, because her small town in Pennsylvania could no longer support a regular newspaper. In part because of the way that social media has changed the average in game.

She starts her own newspaper. Originally it's stories like the birth of her baby brother. Not many people are reading about it beyond the family, but then she starts to cover things that ranged from corruption in the city government, to she reports the very first murder in the town and multiple generations. It's this crazy story and actually it's since been bought to be turned into a Hollywood movie.

The flip side of that is a young girl who was growing up in Palestinian territories on a less bucolic than Pennsylvania. She's grown up surrounded by violence. She's lost family members to violence and she too starts her own online news service, but she describes it as her way of fighting back. She describes herself as not just a journalist, but an online warrior and she seeks out battles to report and she says, "My camera is my gun." This shows to me again, this twin side of what's playing out. There's a rule that how social media has empowered new people, but that rule has both positive and negative stories that play out from that.

[0:12:21.3] JM: As much as I love you turning the question on its head and giving the optimistic take, I'm going to push you back into the dystopic narrative that permeates much of your book. You described several different tactics of LikeWar actors. One of these is a method used in social media where thousands of human trolls are amplified by tens of thousands of bots. It becomes increasingly hard to tell who is a bot and who is a human. Describe how problematic this tactic is.

[0:12:58.7] PWS: The key issue here is that this space, the online space was originally designed for science. Then it was turned into fun. Then it became for-profit. The spaces, whether it's Facebook, Twitter, YouTube, Google, you name it, as result they are designed not for veracity, but for virality. They're designed to draw us in and make us use them more and more.

That has been turned on its head by actors who understand how the space works and attempt to weaponize it to achieve their own goals. That example that you give for instance of creating false personas, what we call sock puppet accounts, and then combining them with bots, algorithms that act as if they're real online. That combination can be incredibly powerful, because it essentially manipulates the network's own algorithms to drive messages viral, that otherwise would not go viral. Which in turn, creates beliefs that would otherwise not be so widespread, new truths, to it can ripple out beyond the social networks.

What is trending online then shapes what other media cover. For example, 97% of journalists use social media to decide everything from what stories they cover, to what angle to take on the stories, to who to interview. Even if you're not on social media, you're listening to the radio, you're watching a cable news TV show. You're shaped by what's going on online and of course, it's not much of it, if you have this manipulation possible, it means it's not authentic.

Early groups realized this. Examples we cover in the book range from of course, the now infamous Russian disinformation activities, where this mix of sock puppet and bot accounts as I mentioned was widespread, highly influential. Again, not just on Facebook. You could see the same playing out on Instagram, YouTube, Twitter of course. One of the accounts we illustrate within the book is one called Tennessee GOP. It was claimed to be a Tennessee Republican who wanted to take their country back. Of course, now we know it was a Russian information warfare account.

That one account, that single account was the seventh most read account on Election Day 2016. Not the seventh most read of the more than 3,000 Russian sock puppet accounts, the seventh most read overall. Those very same tactics were used by Isis for instance, to drive its messages viral. We illustrate how in the Battle of Mosul, Isis had a much smaller physical

invasion force. It had about 2,500 soldiers that are invading against a defending force on the Iraqi army side of about 20,000; one to 10 disadvantage.

Through similarly a mix of bots and sock puppets, Isis drives its messaging viral, it makes it itself appear as if it's winning, controls the narrative online and then the Iraqi soldiers are reading in their smartphones and they believe it and then they run away.

We've seen this move into everything from celebrities and marketing campaigns for products. Again, the product might be a movie. There was a wonderful recent story about how Lady Gaga fans mimicked the Russian disinformation warfare campaign to go after rival movies that were coming out the same weekend as her new movie. A fun amusing story. If you were the producers of those other movies, you didn't like it.

Again, there's no there's a history to this. One of the examples in the book politically is the practice of what's known as Astroturfing, where you have grass roots movements, where people truly do organize to support something. Then Astroturfing is where you create the false sense of a phenomena. One of the ones that's mentioned in the book is Newt Gingrich when he ran for president in 2012. This is reported and not just us saying this over a million fake followers. It creates a sense of there's this massive online following for his ideas.

If you remember, one of the ones he promised was a moon base by the year 2020. That did not get the support, but by creating this Astroturf phenomena makes them appear more popular than they truly are. Again, that's selling a political product but the same thing can be done in the physical products that you buy.

[SPONSOR MESSAGE]

[0:18:19.8] JM: Software engineering boot camps are an alternative to the traditional computer science education process. I've seen several close friends go through a boot camp and find a job as an engineer shortly after. Boot camps are much cheaper than a college education. I see so many engineers coming out of boot camps despite starting the boot camp without much experience as a programmer.

App Academy is a 12-week boot camp where you will learn all the skills that you need to begin a career as a web developer. App Academy teaches you Ruby on Rails, JavaScript and React and you don't need any programming experience to get started with a coding boot camp like App Academy.

App Academy doesn't charge tuition, until a student is hired and earning more than \$50,000 in compensation. Go to softwareengineeringdaily.com/appacademy and find out more about App Academy and apply to get into the program. You will get \$250 off your tuition when you enter SEDAILY in the field for how did you hear about App Academy.

Software engineering is a growing field and app Academy will teach you a great base of disciplines and software engineering practices and skills and tactics that you need to succeed. In only three months, students graduate from App Academy and find jobs at places such as Google, Facebook and Dropbox.

The average starting salary for an app Academy student is over \$100,000. Of course, it's not easy to make it through App Academy. It's not easy to make it through any boot camp, that's why it's called a boot camp, but that's also how they are able to pack so much information into three months. It's grueling. It's really interesting and intense. I've met a lot of people who have said that the condensed boot camp process is one of the most informative periods in their life. If you are looking to learn engineering, it's a great option.

Go to softwareengineeringdaily.com/appacademy to apply and get \$250 off your tuition by mentioning SEDAILY in the how did you hear about App Academy box. Thanks to app Academy for being a sponsor of Software Engineering Daily.

[INTERVIEW CONTINUED]

[0:20:52.4] JM: What's the role of traditional news organizations that have this reputation as being a bastion of trust, place like the New York Times, or perhaps Bloomberg, maybe Vox. What is their role in this new disruptive world of LikeWar?

[0:21:13.0] PWS: Well, a couple things; one is some percentage of your listeners just heard those examples that you said and said, "No way. Those are artisan examples." They knew. They

angry by that. One of the phenomena, part of that belief is a result of how social media has reordered not just our world views. One of the things we break down in the book is how we've organized into – there's a there's a phenomena called homophily, love of self.

Basically again, because of the way the networks are organized, you are more likely to click on, more likely to share stories that reinforce your worldview. We tend to then cluster into different little information bubbles. What's been fascinating then is how you can break down what media outlets are thriving or not within these now more partisan bubbles.

What's been fascinating is on the left, there's still a plurality. If you map it out, there are sort of what people with left-leaning views are reading and what they're sharing online, there's a pretty strong mix. You've got the New York Times, as you've got the Huffington Post. It's like a galaxy with lots of different little universes out there, if you imagine that map.

By contrast, on the right you have the same filter bubble. Both sides are being struck by this, but it has a very different clustering. Essentially, there's a smaller number of universes where it's a hub primarily around Breitbart and then by and Fox News. They tend to link into that.

Two information bubbles, but very different information bubbles. That we've seen – what I'm getting at is we've seen media universe affected by that. In turn, one of the challenges is that some outlets have embraced that new reality and run with it and have used it to drive towards more profits. Breitbart is a good illustration of that. I don't mean good in terms of I'm praising their content. I'm just saying they leaned into the virality side of that. Some don't realize when they're being manipulated.

A good example of something that the companies, particularly in the media side need to catch up to is the fact that over 60% of the articles that we share online, we don't read the contents of them. We are sharing them and taking them in based solely on what the headline is. We're sharing them for a lot of different reasons, because we believe it, or we believe it will influence the outcome of again, an election, or it's a way of signaling about who we are.

The point is that if you can get your lie into the headline, you win. You see this something that it's amazing that still two years after the 2016 election, you see for example, AP and Reuters are

really bad at this. They'll just quote someone who is making an obvious lie; the president is one of these, and then not put any context on it. It'll be the president saying something that is definitely not true. It's not an inarguable thing, but yet it'll be Trump says X. Trump says we can think of all sorts of examples of that. Mexico has agreed to pay for the wall. No, they haven't. That's just simply not true.

They'll just have that quote and that quote again, 60% of the times it's being shared, that quote is getting out there. It's one of these things that companies have both been changed by the marketplace, but also some failed to realize how the marketplace has changed.

[0:25:06.7] JM: Now my personal media consumption has changed a lot since this election, in and trying to come to terms with the sense of unmooring from a shared reality. I feel we have entered a world where it's almost a choose-your-own-adventure for what your reality is. You can just choose what reality you want to live in and you can find media sources and podcasts and audiobooks that reinforce that world.

[0:25:43.4] PWS: If I can interrupt you, it's not just that you can find it. It's that the structure of the networks, the way they work is it will be fed to you. If you think about, for example YouTube, which again, one of the things you need to particularly is the different generations media consumption. For example, if you or I were doing a school report back in the day, we would not have not gone to YouTube. We're being given a report on – write a report on the federal reserve, right? We would have gone to the encyclopedia, or whatever back in the day. I'm dating myself.

The point is if you are a 15-year-old right now, one of the places you would turn to is YouTube, and you would just put in federal reserve. Then besides whatever pops up initially, running along the right of it would be all these other suggestions and you would then click on those and then you would click on the other ones along that. Very soon, you would be down a conspiracy theory rabbit hole. You would be pushed all these crazy ideas that are not true, but just the way the network's own algorithms work if that would happen.

The same thing happens and quite dangerously issues related to extremism, terrorism recruiting, or the like. That's one of the things that the companies have been, I'll say wrestling with is that they design them in this way. Then now they're being called out on that and they are

mixed trying to do things about it, but also it's at the core of how the whole system works. That's how they make money.

[0:27:19.0] JM: This illustrates a few points of why I think podcasts are gaining in popularity; one is that podcasts are based on a pretty archaic fragmented ecosystem of sharing audio content. Your podcast player, I don't know if you're a podcast listener, but it's a chronologically ordered – it's not a recommendation system, and so you just see what is being published in order. In addition to that, the format of the most popular podcasts is a very long conversation.

It's a long-form conversation, oftentimes unedited. It resembles what we might experience in a long-form real-world dialogue. I think it does a good job of sometimes setting an example for how people can have real-world conversations, where people can really dig into ideas. I think of it as a refuge from some of the online notions of conversation.

Have you taken any countermeasures in your personal life as you've realized how damaging the social media ushering of your mind through whatever marketing vortex? Mark Zuckerberg wants to take you through. What have you done in your personal life, your social media habits, or your conversational habits to accommodate the series of changes?

[0:28:42.6] PWS: I want to hit though that point that you're making about podcasts, because it connects to one of the key lessons of the book, is that we wanted to in essence, figure out what were the new rules of the game. As we talked about earlier, you had this wild diversity of actors, whether it's Trump or Taylor Swift or Isis or the Wendy's hamburger chain. Even though they were wildly different, we kept seeing similar tactics. We kept seeing similar phenomena, because they're all playing in the same space.

One of the issues that the book wrestle with was okay, when things go viral, why is that? What are the attributes that they have? The attribute is not that it's true, but there are other attributes that they have that work, so to speak online. We break them down. There's five different ones. One of them is authenticity, planned authenticity.

Authenticity, this is something that we saw whether it was Taylor Swift or Isis's top recruiter. It's the idea that again, it sounds like a contradiction. It's the battle to be real, but being conscious of

the fact that there is a battle to be real. For example, Taylor Swift does what's known as Taylerking. She came up with the name herself, where it really is her. She will lurk around her fansite. She'll see what they're talking about and then she'll link in. She'll for example, congratulate a fan who passed their driver's license. She'll console a fan who broke up with her boyfriend.

What she's doing is she's understanding that this is a space that allow simultaneous mass broadcast, but one-on-one connection. She's having a one-on-one engagement, but in full knowledge that it can be shared with the wider world. It's very similar to what Junaid was saying who is this interesting guy who was interesting/dastardly guy, who was Isis's top recruiter. He was a failed rapper, who later turns to extremism.

I find that to be one of the illustrations of a podcast and why podcasting has taken off, because there's an authenticity to it. It really is you. You and I are having a one-on-one conversation, but it's simultaneously something that can be broadcast with the world and shared with the world. It's done in a manner that's I'm more organic than the very clearly canned version of someone on a TV show, or the like.

Anyone can create their own podcast so that it's one of the other elements of it. It's democratized. That's an illustration of some of the rules that the book breaks down that again apply whether you are running a political campaign, or running a marketing campaign for your small software company. This gets to the direct answer to your question, which is part of what I've changed and what I hope other people are able to change is the recognition that we're all players in this.

If we are online, we are targets of these tactics. We are participants. Our clicks determine whether they go viral or not, whether they get shared or not. That's really important not just in shaping the overall web trends, but whether our friends and family is exposed to them. The key for whether a news article is shared is not whether it's true or not, it's whether a friend or family member shared it.

What I'm getting at is that these tactics are happening whether we are aware of them or not. It's just our awareness. We're either ignorant players in these battles and we're taking advantage of

and we're allowing our friends and family to be taken advantage of, or we understand the new rules of the game and we can react to them. Tilt them back to our previous conversation, tilt them more to the good side, rather than the bad side of the phenomena.

[0:32:41.3] JM: There are engineers that are listening to this right now and they're wondering, "Okay, this is a nice conversation, but what does this have to do with software engineering? Why is this on Software Engineering Daily?" The reason you're an important –

[0:32:52.9] PWS: You guys create the network. You run the network.

[0:32:55.9] JM: That's right.

[0:32:57.0] PWS: You are not just targets of all of these. You are participants in a way that's different. One of the other issues that I found fascinating is you pull back on this, some of the most powerful actors in war and politics today are basically tech geeks, who originally weren't all that interested in war and politics and yet, they're shaping what goes on. You think of Zuckerberg and the wider network of people working in a company like Facebook and then its broader empire.

Zuckerberg gets into this, because he writes really cool software that initially is just about rating whether his dorm roommates and schoolmates are hot or not. That's the origin of Facemash. It's just a good software. He turns it into a business. Now Zuckerberg is making decisions about that shape everything from the outcome of elections to whether genocide happens or not. It's this incredible power, and so you see that plays out at all sorts of different companies, large and small. Software engineers are now powerful players in war, politics, news.

I think we're seeing a coming to grips with that power. I mean, the implications of that and how it can be used for good or ill. We can no longer act like we're neutral, like we have nothing to do that, because even if you take that neutral position, that's taking a position.

[0:34:25.0] JM: I mean, some people have a much more cynical outlook on this, but I don't think Zuckerberg wants people to be dying in genocides. I think he has stumbled into a world of even more power than he imagined, or he craved. It's not just a power in the sense that he can direct

history, it's more a power in terms of he makes decisions and there's a magnitude to those decisions.

The engineers at these companies that he's – like the engineers at Facebook that he's directing, they've been working on solving some of the problems that you outlined in the book. My sense is that the countermeasures to some of these LikeWar negative outcomes have not been very successful. What's your sense of the success of countermeasures against some of these LikeWar tactics?

[0:35:19.6] PWS: A couple of things there. I think first, you're exactly right. You're hitting this transition that the companies and the individuals within them are going through, where I liken it to parents going through the stages of grief. Initially, there was denial of for example, Zuckerberg saying it's a quote, pretty crazy idea that disinformation could have played out on his network on scale and influenced people's actions. The irony is he's saying that back in 2016, at the very same moment that the company is marketing itself to political campaigns as the best place to influence people's actions, in that case their votes.

They've gone from that denial. Similarly, well we don't want to be an arbiter of truth or whatever this pull back. It's not our job. It's not our role. We don't want this. To now they're in the position, if you go from denial to bargaining, Facebook saying, “Nothing was happening too now. We've created a war room to deal with election interference. We're engaged in a ‘arms race’ against Russian disinformation warriors.”

Part of them extolling all those things that they're doing is also saying to politics, governments, their users, “Hey, don't worry. Don't intervene. This is worth doing, so you don't have to force us to do more.” My own personal take is there's some things that they're doing, but they're still a long way for them to go. I think the more and more news comes out, the more and more we can appreciate that.

Part of this is to recognize they're running what is simultaneously a communication space, a marketplace. That's what the internet and in particular, social media has become. It is also a battle space. It is a battle space where these what we call LikeWars, these battles to drive ideas

viral through likes and lies play out every day. By it being a battle space, there will always be a back and forth.

Whatever measure they put into place now, some adversary is going to react to them and try and move around them. For example, mid-Facebook we've seen them put into place measures against Russian disinformation campaigns that frankly if they had been in place in 2016, we'd be in a very different world. Not just talking about US side, to I'd to the level of activity in Brexit. One-third of the online conversation related to Brexit back in 2016 was by inauthentic voices, was by false accounts; one-third of it.

The point is they put those measures in, it's not as easy in 20 – you and I are talking in the very last weeks of 2018, the things, the tactics that were done in 2016 harder to pull off in 2018, but that doesn't mean that the Russian said, "Gosh, I guess we're done. We give up." No, they've just moved on to other new tactics. This is what the companies again are challenged by, wrestling with is that, "Hold it. I'm running a battle space where there will always be this back and forth. Whoa, that's not the job that I set out to have. I set out to create cool tech and make money." I'm sorry, that's part of what's played out.

[SPONSOR MESSAGE]

[0:38:44.6] JM: DigitalOcean is a reliable, easy-to-use cloud provider. I've used DigitalOcean for years, whenever I want to get an application off the ground quickly. I've always loved the focus on user experience, the great documentation and the simple user interface. More and more people are finding out about DigitalOcean and realizing that DigitalOcean is perfect for their application workloads.

This year, DigitalOcean is making that even easier with new node types. A \$15 flexible droplet that can mix and match different configurations of CPU and RAM to get the perfect amount of resources for your application. There are also CPU-optimized droplets perfect for highly active frontend servers, or CI/CD workloads.

Running on the cloud can get expensive, which is why DigitalOcean makes it easy to choose the right size instance. The prices on standard instances have gone down too. You can check

out all their new deals by going to do.co/sedaily. As a bonus to our listeners, you will get a \$100 in credit to use over 60 days. That's a lot of money to experiment with.

You can make a \$100 go pretty far on DigitalOcean. You can use the credit for hosting, or infrastructure and that includes load balancers, object storage, DigitalOcean spaces is a great new product that provides object storage, and of course computation. Get your free \$100 credit at do.co/sedaily. Thanks to DigitalOcean for being a sponsor.

The co-founder of DigitalOcean Moisey Uretsky was one of the first people I interviewed and his interview was really inspirational for me, so I've always thought of DigitalOcean as a pretty inspirational company. Thank you, DigitalOcean.

[INTERVIEW CONTINUED]

[0:40:52.3] JM: In terms of the techniques that are actually being used by these companies to combat some of the problematic conflict behavior, the typical technique that I hear is you combine human labeling with trained machine learning models. I've heard you suggest that AI is not going to be a silver bullet to solving this problem. Can you explain more specifically what your perspective is on the shortcomings of this strategy?

[0:41:24.0] PWS: It goes back to what we were talking about of recognizing the battlespace nature of this and also the twin nature of the good and the bad. We are seeing a greater use of increasingly sophisticated algorithms, particularly it falls under the idea of AI. They are being used for both good and bad purposes, even when creating false personas online.

This mixes everything from what are known as chatbots and then madcoms to deep fakes. Chatbots and madcoms, it's for example an account that can have a conversation with you, even though it's not a real person. They're getting better and better at it, to deep fakes is using AI to create a hyper-realistic imagery that becomes almost impossible for a human to tell whether it's real or fake.

The good examples of these, the companies love them, they're being developed for marketing. It's a lot easier to sell you in this way to – help desks when you've got a problem, you interact first with a machine rather than a human to entertainment; people blending deep fakes in to

make more interesting videos. We've seen this of everything from someone did this to the Star Wars movie Solo, to people have done it with porn movies.

Those aspects is happening, because people think it's going to save money for the company, or make money, or whatever. Then the flipside is of course, it can be weaponized. It can be used for bad ends. It can be used to create – to trick people into voting for things that they wouldn't otherwise. It can trick people into believing something that's not true, manipulating people.

For the companies, you got this twin nature. In turn, increasingly the only way to detect these hyper-realistic fakery is equally through AI. You have this wonderfully science fiction-like outcome, where the future of marketing battles to actual online political battles will be to AI battling with us poor humans in the middle, which is basically the story of the Terminator movies, right? The two robots at the end battling and with us poor humans in the middle.

[0:43:49.2] JM: Do you see any alternative measures? I mean, there's things maybe we could mandate a real identity system for the internet, or we could we could de-platform more people.

[0:44:00.5] PWS: Oh, there's lots of different things that the companies and the policy world and you and I can do about this. We break them down in the book, but one example related to this idea of fakery has been pushed by Senator Mark Warner. Essentially he said, okay companies if you are not going to rein this in for a variety of reasons, including because you see it as in your own incentives to allow it, on the policy side we can't force you to ban at all, but we can maybe say you have to label it. We'll require you to label it.

I jokingly call this the Bladerunner rule, to make another science fiction parallel; the idea that we humans online should have the right to know whether we're interacting with a robot, with a bot, or not. We may not be able to prevent there from being these bots, but we should at least have the right to know it, that labeling system. More broadly when we move out of this idea of fakery, you mentioned the idea of deep platforming. This is one of the issues that has become you have freedom of speech. You do not have the right to push disinformation in a manner that harm society as a whole, even more so to do it knowingly and repeatedly.

The companies have to again, wrestle with this, that there are actors on their networks who are trying to both manipulate their networks and target their users with harm. One of the most interesting things is that now we have the ability to figure out who these players are. One of the most fascinating is that when you map out the spread of three different kinds of ills, conspiracy theory, the second type hate and extremism, and the third type foreign government disinformation campaigns targeting democracies.

One of the things that's fascinating is that you find an overlap between the key, we call them super spreaders, or if you think about a public-health parallel when disease spreads, not everyone's equal. There's almost always a small number of people that are behind a large number of cases of the spread. It's the same thing in these pandemics of conspiracy theory, hate and disinformation.

What's fascinating is that there's an overlap. For instance, one of the key figures behind pizzagate, this crazy, cookie, definitively false idea that there was a secret sex dungeon at a DC pizza restaurant; it goes viral though and actually, this guy believes it and drives up from North Carolina with a gun and conducts a shooting in that pizza restaurant, all driven by this conspiracy theory.

Well, one of the key guys behind the spread of it actually was flipped over if you're looking at the Russian government disinformation campaign of all the people in the world that the Russians decided to echo chamber, to retweet out, to have their bots push out their messaging of all the people in the world. If I remember the data correctly, he was the third most. By several orders of magnitude compared to the eighth, ninth and life.

Basically, the Russians in seeking to harm US democracy and British democracy and the like, said of all the people we want to amplify the most, it's this pizzagate conspiracy theory. The point being to your deplatform an example. If we can figure out how to deal with this relatively small number of knowing bad actors, we'll be able to knock out a lot of the bad thing. Of course, that's not a government issue, that's the company's own decision-making.

Of course, but it also turns to us. We decide whether these very same actors thrive or not. This same actor is out there continuing to push all sorts of other cockamamie ideas. His history

should follow him. Every time he pushes some other crazy idea it should be, “Hey, you were the dude behind pizzagate. You don't get to do this,” joking to them to make a pop-culture reference. It should be in with the North in Game of Thrones. We should never forget. It should always be there.

[0:48:25.6] JM: Yeah, I'm with you there. I think, this is all the more reason to encourage there to be more social networks, such that when somebody gets “deplatformed,” they at least do have some other place to go. Maybe they shouldn't be welcome on the public square of Twitter, but there's other social media platforms they can go to. There's other forms of monetization they can reach. They should go to those places.

[0:48:52.3] PWS: Again, you have a right to free speech. You do not have a right to use a privately-owned network to violate its own created rules and to push false information designed to harm society. You can go stand on your little wooden box on a street corner, but that does not mean you have a right to use these networks.

Again, that's not me making this up. That is the way the law has come down on it. What the companies we've seen them go from saying, “No, we don't have to make this decision.” To now they are starting to wrestle with that. You look at the example of someone like Alex Jones. Alex Jones behaved in the very same way three years ago that he behaved about five months ago. Effectively, the company is changing their minds, because of people like you and I, the user base decided what this activity is we don't like it. We don't want it to be on our network. If you continue to allow people to do things, like for example, push false messages where you think of – it's not just Lizard Men and stuff like that.

He was knowingly and consciously spreading false information designed to cause harm to for example, the parents of the kids who'd lost literally kindergarteners killed in mass shootings and he's pushing out information that he knows will cause them harm. The company's basically changed their mind and as you know, they deplatformed him. They say, “You know what? We're no longer allowing you to do this.” It has a very real effect on his business model. That's one of the other things to remember about all this, it's a business. Any time there's the spread of a conspiracy theory of the like, there is someone who is profiting from it. If you understand that,

then you're less likely to be taken in by the conspiracy theory and also shapes what we can do about them.

[0:50:58.4] JM: Okay. The subject of China. In China, the government pays civilians to post positive things about the government on social media. I spent some time in China recently. I went to a conference. My first-hand experience was in contrast to some of the perception that I had gotten from the internet, which had convinced me that China was I guess more closed-minded, or had at least a different, more restrained sense of what they wanted than people from the United States.

In China, I really felt there's a shopping mall in every corner, there's Starbucks and KFC everywhere. It felt like New York. I got the sense that the Chinese want what we want. They want peace and consumerism and art and technology, but the public narrative is that we are fundamentally different than the Chinese. How different are we from the Chinese and how does the social media LikeWar manifest in China?

[0:51:59.3] PWS: What you're putting your finger on is how the internet itself is changing. We have this notion of this shared information space, global and the like. Yet, it's becoming broken down into you might think of it as fundamentally different internet experiences based on where you are geographically. If you are in the United States, there are certain social media platforms that are incredibly popular and they control the rules of the game.

If you are in Europe, those very same social media platforms are popular, but the government is put into place different rules that shape what is allowed or not on them, in a way that is not possible in the US political system right now. If you are in Russia, there are other social media platforms that are popular; VK, instead of Facebook.

The government is using its power to control what is on them and means that would not happen in Western Europe or the United States. For example, VK essentially the government forced the buyout. They threatened the young owner, the Russian version of Mark Zuckerberg. They threatened him with various prosecutions, chased him away from the country and the company was sold to a Putin crony.

If you live in China, other companies that are popular and as you know embrace, if you're particularly in the urban areas, use of social media and digital commerce combined together in a way that way more – you would describe futuristic than in the United States. It's like your Facebook and Amazon and Yelp, everything smashed together into one platform all there together. Then you combine that with a government that is an authoritarian government and is using that mass scale of data to control the populace in a manner that would be unthinkable not just the United States, but unthinkable to even someone like George Orwell.

You have everything from web screening, where you may have mass internet use, but there are certain terms and ideas that simply can't be typed. It will not appear on the internet. Try and find something about Tiananmen Square, to for a period of time as we joke about in the book, joke but it's real, Winnie the Pooh was screened out, because people were using it as a way to talk about the Chinese leader. He had a waddle like Winnie the Pooh. The government responds by cleansing the web of Winnie the Pooh.

To as you know, you then also have the use of cheerleading, government paid folks, sometimes it's called the 50 Cent army, who essentially they push certain party lines and drive that good news viral on scale, to you have the social credit system that's emerging, which basically it's a – the idea ultimately when it's put into place is that people will get a single numeric score of their trustworthiness in the idea of – in the mind of the government in this corporate makeup, where your single score will reflect all of the different activities that you do.

For example, if you buy diapers online, your score goes up. You're a good parent. If you play video games too long, your score goes down. You're screwing around too long. Because it's a network, it's not just your activities, but your friends and family's activities. If your brother says things bad about the government, your score goes down too. That score then shapes all sorts of we might describe them as real-world activities, so you get rewards, free charges at coffee shops, to you might get negative outcomes. If your score is not high enough, you aren't allowed on a plane flight, you don't get a bed on an overnight train, to really creepily it's being woven into things like job applications, to online dating.

If your score in the ideas of the government is not high enough, you will not be matched with someone who is attractive. You can see this fundamentally different internet experience as a

means of government control. Again, the point is that we'll have all of these LikeWars out there, but we may see them play out differently in different geographies because of the politics of this.

By the way, back to the discussion of software engineers, just like the original, called the Great Firewall of China was originally designed by Western tech companies, the same thing the scoring system is drawing from technology that software engineers located around the world, not just in China, helped create. To a great ending point for our conversation, you may not be interested in LikeWar, but you are likely participating in it.

[0:57:05.4] JM: P.W. Singer, thank you for coming back on the show. I really enjoyed your book. I'm looking forward to whatever you come out with next.

[0:57:12.8] PWS: Thank you so much for having me online.

[END OF INTERVIEW]

[0:57:18.5] JM: OpenShift is a Kubernetes platform from Red Hat. OpenShift takes the Kubernetes container orchestration system and adds features that let you build software more quickly. OpenShift includes service discovery, CI/CD, built-in monitoring and health management and scalability.

With OpenShift, you can avoid being locked into any of the particular large cloud providers. You can move your workloads easily between public and private cloud infrastructure, as well as your own on-prem hardware. OpenShift from Red Hat gives you Kubernetes without the complication. Security, log management, container networking, configuration management, you can focus on your application instead of complex Kubernetes issues.

OpenShift is open source technology built to enable everyone to launch their big ideas. Whether you're an engineer at a large enterprise, or a developer getting your startup off the ground, you can check out OpenShift from Red Hat by going to softwareengineeringdaily.com/redhat. That's softwareengineeringdaily.com/redhat.

I remember the earliest shows I did about Kubernetes and trying to understand its potential and what it was for. I remember people saying that this is a platform for building platforms.

Kubernetes was not meant to be used from raw Kubernetes to have a platform as a service. It was meant as a lower level infrastructure piece to build platform as a service on top of, which is why OpenShift came into manifestation. You can check it out by going to softwareengineeringdaily.com/redhat and find out about OpenShift.

[END]