EPISODE 487

[INTRODUCTION]

[0:00:00.6] JM: Military force is powered by software. The drones that are used to kill suspected terrorists can identify those terrorists using the same computer vision tools that are used to identify who was in an Instagram picture. Nuclear facilities in Iran were physically disabled by the military sponsored Stuxnet virus. National intelligence data is collected and processed using the map reduce algorithm.

The military keeps up with technology more effectively than lawmakers. It is common to read a quote from a senator or a judge that shows a basic misunderstanding of cybersecurity. Many politicians do not even use email. There’s a large and growing knowledge gap between military capability and the technological savvy of policymakers. On the whole, government is not prepared for modern warfare. We are lucky that military conflict in 2017 is decentralized. There are small skirmishes in the Middle East, but there's nothing compared to the centralized hostility of World War II. The bonds of international trade forms some protection against a war between major powers like the US and China, but it's easy to imagine circumstances that could lead to global war.

There's an arms race between the United States and China and this arms race is happening in an environment of increasing informational chaos. This informational chaos stretches from the highest levels of government to the least informed of our citizenry. Online journalism is becoming physically dangerous. Journalists are being tracked and threatened. Locations where journalists live have been published by enemies of those journalists and this war on journalists has a chilling effect on the production of truthful information.

In the war between truth and false information, the people promoting false information have a giant advantage, and that advantage is growing, because we cannot identify who was a bot and who is a human.

This is certainly a topic that we have tackled on Software Engineering Daily previously, but in today's episode we can consider the ramifications in potentially inciting a global war, because of so much confusion around how much is a message being promoted online by real people who actually believe that message and how much is being promoted by a bot.

I use social media as just one example of the fog of war around information. There is also a fog of war around cybersecurity attribution and this can create an inability to trace real-world physical violence that is enacted remotely through computers. When the power grid gets knocked off-line by a hacker, how do we know who is responsible? When a drone flies through New York City shooting at people, how do we know who deployed that drone? When self-driving car technology becomes open-source, how long will it be before we see a 9/11 type of event performed remotely with cars instead of an airplane, and when it does happen, how will we respond?

Imagine the level of grief and anger on 9/11 that caused our government to launch a war on Iraq. Whether or not you supported that war, we were at least sort of aiming in the right direction of the geographic location where the attackers came from. What would we do if we could not even figure out who launched such an attack? What would we do if we couldn't have figured out who launched Pearl Harbor's attacks.

When cyber forensics teams look into a problem, it might appear that an attack came from China at one layer, or came from Russia and another layer, or it came from some domestic attack or at another layer. This could be time-consuming. It can take a lot of time to uncover the truth behind a cyber attack.

Just like in social media information wars, the instigators of conflict have an unfair advantage and the ability to instigate such a conflict is democratized. Social media, open-source software and cloud computing give a technologist superpowers. Cryptocurrencies can anonymize the transactions to pay for such tools, and basic encryption can anonymize the terroristic acts that occur over a remote Internet connection.

Peter Warren Singer is a political scientist who formerly worked in the United States advisory committee on international communications and information policy. He's also an author whose books include *Wired for War, Cybersecurity and Cyber War: What Everyone Needs to Kno*w, and *Ghost Fleet: A Novel of the Next World War*.

Peter writes about the circumstances that could lead to global warfare and how military actors might behave in such a third world war. In this episode, Peter shares a dark but realistic vision that we should all hope to avoid.

If you like this episode, we have done many other shows on related topics including drones, IoT security and automotive cybersecurity. To find these old episodes, you can download the Software Engineering Daily for iOS and for Android and you can look at the security tab to find all the security related episodes.

In other podcast players, you can only access the most recent 100 episodes of Software Engineering Daily, and with these apps you can access all 600+ of our back catalog, and we're building a new way to consume content about software engineering. These apps are open-sourced at github.com/softwareengineeringdaily, and if you're looking for an open-source project to get involved with, we'd love to get your help.

With that, let's get on with this episode.

[SPONSOR MESSAGE]

[0:07:35.4] JM: At Software Engineering Daily, we need to keep our metrics reliable. If a botnet started listening to all of our episodes and we had nothing to stop it, our statistics would be corrupted. We would have no way to know whether a listen came from a bot or from a real user. That's why we use Encapsula to stop attackers and improve performance.

When a listener makes a request to play an episode of Software Engineering Daily, Encapsula checks that request before it reaches our servers and filters bot traffic preventing it from ever reaching us. Botnets and DDoS are not just a threat to podcasts. They can impact your application too. Encapsula can protect your API servers and your microservices from responding to unwanted requests.

To try Encapsula for yourself, go to encapsula.com/2017podcasts and get a free enterprise trial of Encapsula. Encapsula's API gives you control over the security and performance of your application and that's true whether you have a complex microservices architecture, or a WordPress site, like Software Engineering Daily.

Encapsula has a global network of over 30 data centers that optimize routing and cacher content. The same network of data centers that is filtering your content for attackers and they're operating as a CDN and they're speeding up your application. They're doing all of these for you and you can try it today for free by going to encapsula.com/2017podcasts, and you can get that free enterprise trial of Encapsula. That's encapsula.com/2017podcasts. Check it out. Thanks again, Encapsula.

[INTERVIEW]

[0:09:23.3] JM: P.W. Singer is a political scientist and the author of several books about modern warfare. Peter, welcome to Software Engineering Daily.

[0:09:30.3] PWS: Thanks for having me.

[0:09:31.8] JM: Your writing explores the state of the world today and how that state of the world might lead to a war. You also survey the weapons systems that will be used in a modern war and the continuous ethical concerns that those modern weapons will lead to. Today, our military conflict is decentralized into small skirmishes that probably feel remote to the average citizen, at least if we're talking in terms of the United States military conflict. The average citizen doesn't really feel like we're at war relative to how they might've felt during World War II.

Describe a scenario that could lead us into a centralized conflict with a major power like China or Russia.

[0:10:17.5] PWS: Sure. A bit of background on myself and where I come at on these projects, so I've written a series of nonfiction books and most relevant to our conversation was one called *Cybersecurity and Cyber War: What Everyone Needs to Know*. That was basically a primer on cybersecurity issues, and then what we did in the book that you're referencing called *Ghost Fleet,* it is a novel of the next world war. It's fiction, but it uses nonfiction in terms of technology and scenarios to explore. So it uses the package of storytelling to look at what the future of war in, say, the 2020s might be particularly as you bring in types of conflict where we truly haven't seen major fighting, but likely will in the future; battles in cyberspace, but also outer, space battles at sea, battles in the air, and that really gets at the heart of your question in terms of what would be different from today, and even the last several generations of conflict.

If you're talking about a conflict against a major state power, against a China, against a Russia as supposed to against a Taliban, an ISIS, a Vietcong, what you would see is you notice this centralized against formal militaries. Militaries not just like Saddam's Iraq, but truly capable, able to go back-and-forth for control in these other spaces. So you would see battles for control of the air, battles for control of the sea, battles for control of cyberspace. What you're talking about as you note is the kind of battles that the United States really hasn't been in for about 75 years since World War II. Go back then, the last time the Air Force fought against the troop here, it was the Army Air Corps, and that really brings in a different type of obviously war fighting. You're also talking about a different way that the nation might be engaged.

Again, the difference though with a World War II and were talking about things like cyberspace is that you wouldn't have these very neat geographic divisions and divide other than the attack on Pearl Harbor, American territory itself wasn't really touched during World War II. You had a couple of like balloon bombs that flew across and tried to hit Oregon, but overall it wasn't hit. If you're talking about cyber conflict, it will inherently touch the home front.

One of the other things that we explore in the book is if you’re talking about cyber conflict, you're talking about a space that’s inherently civilian. It's owned and operated by civilians. So it's not just the targeting might hit assets inside the United States, private companies, infrastructure, you name it, but that the players themselves would be civilian. Again, we use that in the book to both explore this, but it also gives you some really great storytelling opportunities, characters to play with, things like that.

[0:13:18.6] JM: The success of the modern American economy is closely tied with Chinese production. Aren't we interdependent with China? What would make us go to war with China?

[0:13:31.7] PWS: So you're putting your finger on two different things there. The first is the idea that, well, we’re so linked together. We would never go to war. In fact, that was an argument that was made famously in 1913. People looking around and saying there's such a level of global trade like it's never been before. The nations of the world will never go to war. Of course, a year later that happened. Moved forward World War II, France and Germany were each other's greatest trading partners. The United States was Japan's biggest trading partner.

So in history, this idea that if you have a mesh trade with someone else, it will keep you from going to war just doesn't hold true, and therefore we should believe that somehow it's a magic recipe for keeping conflict from happening in the future.

In fact, when you've got these kind of relationships that can lead to the opposite, it can lead to disputes and a like, whatever. The first is the idea that we shouldn't kid ourselves, that we are inherently prevented from going to war with those that we have links to. Again, the reasons for going to war in the future would be the same as in the past. Sometimes nations go to conflict out of some kind of set of deliberate choices. They think that they're being penned in. They think that there's a crisis that they have to take advantage of. They hate the other side. There's a dispute that escalates for whatever reason they decide to go to war.

Often, it has more to do with their own domestic politics than it does external relations. They look for someone else to blame. You name it. Then there's conflicts that start not out of a set of deliberate choices, but they start out with some kind of miscalculation, some kind of accident, some kind of crisis that escalates. There's a comparison between World War II very deliberate set of choices to go to war that on the US side leads to Japan deciding to carry out Pearl Harbor. You can compare that to World War I where you had no one believing that the nations could go to war. This Archduke is killed. None of the leaders in Europe write in their diaries that day, "Oh! Today was the day that the first world war began." Instead, they're writing things like, "Yeah, he was kind of a jerk. It's good to get rid of him. You say it." Over the course of the next month, this idea that war makes no sense suddenly takes on a logic of its own as they miscalculate, as it escalates, you name it.

I think about that when we're looking forward. You look at a conflict with a Russia, with a China. As you and I are talking right now, we've got situations playing out with a North Korea with an Iran. Sometimes the conflicts risk could be someone deciding to go to war. Other times it could just be some bad miscalculation, some kind of accident, something that spins out of control where leaders are not acting wise.

Now, there's another part of this that I want to hit. Your dependence on the other side may not keep the peace, but it does point to certain vulnerabilities that might be taken advantage of, and that's really the difference today from both the kinds of conflicts we've been fighting for the last couple of generations and even those in the past.

Again, an ISIS, a Vietcong, whatever. We did depend — Even a Nazi Germany. We didn't depend on them to manufacture key systems not just on the civilian side, but also on the military side. If we are looking to the future, you have the problem of being dependent on potential adversaries for your systems for their spare parts, basically your supply chain. That's tough enough, but then you have something else that we haven't seen before that's introduced by the space that your podcast is on, which is the notion of not just software vulnerabilities, but hardware vulnerabilities.

We know hardware hacks are possible. We could very well see them in the next conflict. One of the things we play with in Ghost Fleet is the illustration of what does it mean to go to war against another nation that makes over 80% of the microchips that go into your jet fighters?

[SPONSOR MESSAGE]

[INTERVIEW CONTINUED]

[0:18:53.8] JM: Well, and also if we’re looking at the United States from the point of view of China, most of the mobile phones in China run android. Android was originally developed in the United States, perhaps I would find it likely that the United States has more or a significant understanding of android at least and maybe there's some undisclosed vulnerability that the US government knows about, but you could definitely imagine a mutually assured supply chain vulnerability, whether we’re talking about the hardware supply chain that China controls. China shipped its finished hardware to the United States which supports the American hunger for electronics, and a lot of software that originated in America runs on the hardware that is in use in China, but the mutually assured destruction is harder to visualize in a modern context.

In the Cold War, it was very easy to visualize just atomic clouds going up in the entire world being in ruins. With the electronic-based, mutually assured destruction, it seems like it's a little more ephemeral and it's hard to imagine just a single action or a couple single actions leading to a complete destruction. You can imagine much more of a gradient, sort of like what we’re seeing with the gradual information wars developing with more and more misinformation, more and more political bots.

In terms of what scares you the most, in terms of like things that could gradually lead to some sort of major conflict, is there anything that stands out in your most plausible nightmares?

[0:20:43.7] PWS: You’ve touched on so many different things there to hit. The first is this idea of a comparison back to the Cold War into cybersecurity with mutual assured destruction. That comparison, I'm not sure if it works. Notice I was saying there, we are seeing a return to great state power, tension, and competition the way China is a rival politically, militarily, technologically, even in the Olympics in the way that we haven't seen since the Soviet Union, you have that, but you don't have when you're talking about cybersecurity, mutual assured destruction.

Let’s break that down. You don't have mutuality. The United States is far more dependent on the systems than most of our adversaries, not just a China, but a good example would be North Korea. You don't have that kind of mutuality. When you're talking about cyber conflict, when you're talking about cyber-attacks, you also don't have the assurance side. There is just far more uncertainty plugged in as to whether an attack is even happening, to whether the attack is working. The best kind of attacks aren’t evident to the victim and their impact is often tough for the attacker to know about. In fact, it's not just merely that it's not evident. It's that sometimes the best defense is to not let the attacker know that you're aware that you're under attack, because then you can steer the attacker into alleyways where they can't do damage or you can feed them false information, you name it.

Then you hit the destruction side in MAD, mutual assured destruction. That's really the difference of nuclear weapons where there is very clear and catastrophic levels of destruction, versus cyber-attacks, their impact varies. There might be attacks to steal information. There they might be attacks to block the flow of information, DDoS against the bank or what Russia did to Ukraine and their conflict, blocking communication between government websites and military units.

It might be an attack to cause physical damage [inaudible 0:22:56.2] what we did with Stuxnet to sabotage Iranian nuclear systems, but even then the level of physical damage is not going to be to the level that we saw with even a nuclear weapon back in the 1940s. As scary as all the scenarios of cyber conflict are, “Oh! Someone might turn off the power grid,” which, first, haven't seen it done at a mass level, but even if it happened, it still wouldn't have the kind of permanent and catastrophic damage that even a small nuclear weapon would cause.

Those comparisons of MAD don't work as effectively. It also points to how cyber-attack, cyber weapons, unlike nuclear weapons, are something that happens all the time. They are used even before outright wars happen. We’re seeing mass scale cyber-attacks right now, and they can also be used by a wide set of actors, not just powerful states, but my non-states; criminal groups, terrorist groups, individual hacktivist, you name it.

That comparison is not a great one and I think it's one of the challenges of how too often policymakers talk about this viewing cyber-attacks is some kind of — I remember a senator saying, “It’s like a weapon of mass destruction.” Actually, it's not. It's more difficult to frame it that way. Then you put your finger on something else that we've seen, which is that most of our discussion around cyber-attacks, around cybersecurity has been around the idea of hacking a network.

The way a Russia, a China frame it though is that they put it inside a broader context of information operations or influence operations. A different way of putting it is that, it's about packing the people behind the network, and we can see this with what played out targeting the American presidential campaign in 2016, but not just the United States. It's in hit political campaigns in Germany, in France, Britain, you name it, they haven't a just hit political campaigns. They hit topics well beyond.

The point is that it's been not about stealing information and breaking into the network. Again, it's been about going after the people, and I think it's a really fascinating example to see not just for what militaries and governments are dealing with, but even private companies.

Facebook has one of the world's top cybersecurity teams. Great level of expertise, large amounts of investment and they were, to put it bluntly, looking in the wrong place in 2016. They were very naturally, at the time very smartly focusing on people trying to break into their networks to target that in this way. So they weren't looking at, they weren't developing responses for people trying to hack the conversation on their networks, to hack the minds so to speak and opinions of their customers. They were bluntly ill-equipped to handle everything that played out on their networks, and it was only after the —Again, like many of cybersecurity incidents, they didn't have a great level of awareness of it. Then when they first noticed, they kind of down play it. Mark Zuckerberg, for example, as soon after the election, saying things like, "There was not a big problem it." I think his quote was pretty crazy, the idea the fake news would have any impact.

Then very soon after, like what happens in cybersecurity incidents, they had to revise. They had to say, "Actually, remember when we said there wasn't anything going on? Actually, there was. Remember when we said it was really small? Actually, it was really big. Remember when we said it didn't have a big impact? Actually, it had a huge impact."

[0:26:52.2] JM: I think he earnestly believed what he was saying at the time.

[0:26:55.0] PWS: Again, you sort of see this was traditional cybersecurity incidents, and it happened with the influence operations side. Then to the, "Well, what could we have done about it?” There's a great comparison between what was not done to defend the American election versus what was done to defend just a couple of months later, the French election.

Companies like Facebook and Twitter were knocking off-line. I believe it Twitter it was 200 fake accounts and I think it was almost zilch at Facebook before the American election. Before the French election, they took over 40,000 off-line. Now, you can't tell me the Russians cared that much more about the French election. It was actually just a matter of doing something about it.

[0:27:43.0] JM: Now, there is a lack of understanding unfortunately in the government about cybersecurity. In addition to being an author, you were a member of the State Department's advisory committee on international communications and information policy. So you are familiar with how the US government sees cybersecurity.

Just as an example of one of the misunderstandings that people in the government have implemented, is there's this belief about cyber war, that offense is easier to do than defense. This is something that you have alluded to before. The strategy that we take is we invest — I think you said, a talk I saw, like four times as much in offensive capabilities as defensive capabilities. Could you unpack that the notion, that defense verse offense, what should we be investing in?

[0:28:37.6] PWS: Sure. Now, that references a certain particular kind of military spending, but overall it hits this problem as you frame it in terms of cybersecurity and how we look at it, and it's treated either as this sort of mystical thing that people don't have to wrestle with, or often they look for the very simple and easy solution. Again, that's not just a political problems. That happens on the business side too. We can see this in terms of much of the discourse around cybersecurity and cyber war in government, particularly engaging with senior leaders, is this idea of either deterrence. If I just build up my offensive capability, I'll make the bad guys go away. I'll scare them.

As we were just talking about, that’s just not proven to be the case. We know that's not been the case, because the United States has a huge amount of offense of capability. In fact, the people, the NSA have much to be angry with Mr. Snowden, but the one thing they can take away from what he revealed as it showed, we have some pretty incredible offensive capability, and that's not changed. Developed some novel weapons type so to speak, like Stuxnex, to operations, you name it, but did this capability stop the level of cyber-attacks on the United States? No. We haven't seen an appreciable downgrade since the rest the world became aware that we have offensive capabilities if there was any doubt in it.

There's this idea of, "I'll scare the bad guy away," or there's the classic defense idea of, "I'll somehow keep the bad guy out of my networks. I'll have some kind of perimeter fence that will keep them away." The reality is, in both government and on the business side, those are both losing propositions. You're not going to scare all the bad guys away and you're not going to keep all the bad guys out. Heck, the bad guys may already be inside your network. They may be some of your own team. Some of the worst incidents for cybersecurity for the US military, for example, been insider threats, like I referenced, Snowden or Manning, same thing for private business.

Instead, we would get a lot more bang for our buck out of a resilient strategy. Resilience is about accepting the bad thing is likely to happen, that the bad guy is likely to get inside your network. They might already be inside your network. Instead, it's about focusing on powering through that bad day, that bad thing. It's about recovering quickly when you get knocked down. It's about shrugging off the harms. It's about building a capability essentially to achieve what we call deterrence by denial. That if the bad guy isn't going to get what they want out of it, that's more likely to succeed against them.

The important thing about resilience is that it works against any kind of attacker, whether the attacker that's coming against you is a state power, like a China or it's an individual criminal, or a hacktivist, or resilient strategy is good against all of them as supposed to certain kinds of classic deterrence strategy. So I think we'd get a lot more out of it. Similar thing for businesses, you can build — Businesses really can engage in the offense of side. There's been some talk back and forth about giving them powers to hack back, but it's a lot like other forms of vigilantism. It sounds good, but it actually doesn't work. It's more complicated than that. Most focus on the defense side, keeping the bad guys out. Again, I just think from a resilient strategy, they're going to get more bang for your buck.

The problem of it is that it's a lot easier to sell someone. Politically, you're on the business side, some kind of silver bullet, tough guy sounding strategy, “I'll punish the bad guy,” or “I’ll buy my widget and the bag will never get inside your network,” or “give me the authority and I'll solve your problems for you,” as supposed to resilient strategy, it's not as sexy. It’s saying, “Look. The bad thing is likely to happen. This is what we can do to mitigate it.” It’s like trying to sell insurance even though we all know insurance is what we need, but we'd rather go after that sort of magic bean.

[0:33:14.1] JM: Yeah, and as you've said, even the advanced adversaries, like state actors, are using fairly simple techniques, things that could be prevented by updating your software on a regular basis or using some very standardized endpoint security techniques, so much low hanging fruit, and you can imagine that low hanging fruit, if you just invested enough money and gave it to the right people to implement it, then the infrastructure that we depend on would become a lot more secure.

[0:33:50.3] PWS: Yeah, and you framed it exactly right. A lot more secure. Not perfectly secure, but a lot more. We’re often our worst enemies, and that we want some kind of perfect solution. So that idea what you're hitting on is cyber hygiene. When we can think about cyber hygiene, if the individual user level, “Don't click on those links you ought not to. Change your passwords,” to cyber hygiene in terms of best practices and setting up networks and information sharing, you name it. You'll often hear people say things like, “Yeah, but at the end of the day someone's going to click that link.” You’re like, “Yeah, that will happen, but we can shrink that number. We can make it less of a harm. We’re never going to prevent everything, but we can reduce it. That'll allow the defender to spend more time on the complex task as supposed to the low hanging fruit times.

I like the hygiene parallel, because it's a lot like in public health. No one thinks that covering your mouth when you cough or washing your hands are going to prevent all diseases, but it helps a lot, and it means that we’re not having to deal with as much of the sort of low level stuff. I think there's a lot to pull from that in terms of best way to use resources, but also about managing our expectations.

[SPONSOR MESSAGE]

[0:35:23.3] JM: GrammaTech CodeSonar helps development teams improve code quality with static analysis. It helps flag issues early in the development process, allowing developers to release better code faster.

CodeSonar can easily be integrated into any development process. CodeSonar performs advanced static analysis of C, C++, Java, and even raw binary code. CodeSonar performs unique data flow and symbolic execution analysis to aggressively scan for problems in your code. Just like battleships uses sonar to detect objects deep underwater, engineers use CodeSonar to detect subtle problems deep within their code.

Go to go.grammatech.com/sedaily to get your free 30-day trial exclusively for Software Engineering Daily listeners. CodeSonar analyzes your code and it delivers a detailed report. The CodeSonar user interface provides all the information that you need to quickly understand the reports. Follow cross-functional paths, understand cross-references, quickly navigate between files and visualize large pieces of your code.

Go to go.grammatech.com/sedaily to get your 30-day free trial and unleash the power of advanced static analysis.

Thanks to GammaTech for being a sponsor of Software Engineering Daily.

[INTERVIEW CONTINUED]

[0:37:02.8] JM: As far as the private sector, we have had companies in the private sector that provide military technology to the US government for decades, and obviously there's well-known military contractors like Raytheon or Lockheed Martin, but today you see, for example, Amazon has a data center that's completely devoted to, I believe, the — Maybe not the NSA, but I think it’s just government related stuff. Who are the companies that provide military technology to the US today? What's changing in the relationship between private sector and the public sector?

[0:37:44.6] PWS: I think you’ve seen a series of changes. One — And think of them as sort of different types of directions. One is not traditionally viewed defense contractors providing some kind of service that is now could be viewed in a traditional way as inherently military or inherently governmental. A good example might be cloud services, where we've seen everything from you name your business, travel agency, hospital, to CIA and the Pentagon all making use of this and seeing it as not just a way to achieve efficiency, but as potentially a way to achieve better security.

You see the opposite direction happening though as well where there are traditionally defense companies that have developed a military grade, so to speak, level of cybersecurity expertise that they're going, "Hold it! Actually, we can and arguably should sell this to other parts of the private sector, because they're getting hit by the very same attackers using the very same techniques. In some cases, it was because the defense contractors developed a product to sell to the military, or in other cases it's because they were among the very first to be targeted by these advanced persistent threats, so they developed certain capabilities to defend their own corporate networks and then they realize, "Hold it! Actually, we could sell this to others that are being hit by this that are outside the defense industry," but we're still seeing this kind of targeting. You see that going on.

Then there's the part that we were talking about before, which is the kind of global multinational nature of really just business writ large, where it's very difficult now to identify companies that if they are of scale that are American, so to speak. They're American. They may have been founded in America or their corporate headquarters are located in America, but they will be doing business all around the world. Their shares are owned by folks all around the world, and we could see the impact of this after the Snowden affair where you see certain companies acting as global entities, not as just purely an American entity sand they see that is necessary to their future prosperity, but of course go back to what we're talking about of be it supply chain management issues or be it something related to a potential future conflict. The way in a World War II that a Ford says, "No. We're an American company. We're going to be the arsenal of democracy."

Would certain companies in the 21st century, if there was a conflict to outbreak between a U.S. and a China, how would they navigate that? How would they decide? Would they make the decision based on where they were founded? Would they make the decision based on where their primary marketplaces were? Would they make the decision based on what their shareholders decided? Again, you can sort of play this out and it's an interesting question that would have to be explored.

[0:41:09.2] JM: Another area that is going to be fought over in a modern digital battlefield, is that of finance and banking, and maybe even cryptocurrencies? Do you consider the role that Bitcoin and/or the banking system might play in a modern war?

[0:41:30.6] PWS: Gosh! I think that there's a couple of things. The first is to debunk a lot of the hype that surrounds these technologies. Let me clear. They are important. They are revolutionary. They're historic in terms of the notion of how currency value itself was once some mineral that was mined, gem, stone, gold. Then it was turned into a coin that was backed by a certain government, and then it was valued by how much gold was in that coin. Then it was, “No. No. No. It's a piece of paper and it's the pledge of the government behind it that matters.” Then it became electrons that a government was backing. Then now it's the potential of something virtual. So it's a very big deal, but there's a caveat I just want to put on it.

There're so many different articles that are out there that are how this certain technology, and it might be the currency version of it, Bitcoin or it might be kind of the broader technology blockchain where it's like, “This is the solution to,” and then you insert whatever problem. It's a solution to poverty. It's a solution to global health. You're like, “No. It's not going to be the solution to that. Let's cap the hype,” or some of the idea that it's unhackable. Sorry. We've already seen people go after these marketplaces. So it's important, but we need to remember it still happening within.

[0:43:00.4] JM: Sorry. I probably should've disambiguated the question a little bit more, because I'm completely with you, but let's play out Bbitcoin like 5, 10 years and let's say Bitcoin starts to become a more appealing currency than something government backed. Let's say certain currency start to get debased relative to Bitcoin. Do you think that sort of financial fluctuation could spur a conflict?

[0:43:28.4] PWS: I don't know. You and I could certainly spin up a good story around that, right? We could spin up a story about how it would stop conflict, that the governments of the world wouldn't be able to fund their wars or the ultimate Bitcoin entrepreneur would be able to threaten to shock economies if they wanted to go to war. We could also spin up the exact opposite story, that it creates a kind of challenge or even crisis for governments, and what do governments often do when they face a crisis or a challenge? They look for scapegoats. They look for ways to mobilize their population to blame something or someone else. We could do both of those.

There's also into what we've already seen, which is that these technologies have their use, because they're useful and particularly they bring efficiency to certain marketplaces. By the way, they've also brought efficiency to the marketplace of cyber threats. They've made it easier for attackers to coordinate to trade capability, and so they’re great, but they've also made it easier for bad stuff to happen too. We could spin lots of different stories around them, and I think that's what illustrates how important they are, but I also — Kind of the caveat I was trying to do around it, is we sometimes forget about all the other things that surround the technology, the politics, the people, the law, the marketplaces.

[0:45:01.3] JM: Yeah. At least we have touched on the role of fiction which I have also heard you talk about, so I won't have to ask you about the importance of fiction. We've already just illustrated that. Let's talk about more contemporary threats instead of fanciful things like the threat of a cryptocurrency destabilizing the world. We have set a certain precedent for the way that drones can be used in military conflict. Have we set a dangerous precedent or have we been intelligent and measured in how we’ve set a precedent about drone usage?

[0:45:40.7] PWS: I think more towards the former than the latter. We assumed that we were — The exception and then we could also set rules that others would follow, and that's just proven not to be the case. Let me be clear, there's a difference between using the technology and then the ways that you use it. This idea that it's not about whether to use robotics or not. That's already happening.

It’s funny, I was having a conversation today with people around — There are some people who still make arguments, “How do we prevent the proliferation of armed drones.” My answer is, “Do you have a time machine, because it's already happened.” The United States is not the only player in this space. 86 militaries have robotics systems. Well over 30 of them are armed ones and they range from US allies, like in Israel, to potential adversaries, like China or an Iran to ones that are those problematic in the middle, the frenemy's, like a Pakistan that's both an ally but has been a problematic ally for us to put it kindly.

We've already seen the proliferation, the technology. Then, “Okay. What are the rules for how you're going to use it? There's one aspect of using on a clear and defined battlefield and having it follow the laws of war. Then there are other problems in terms of, “Well, when I start to use them outside of war zones. What about when I start to use them to carry out strikes that generically people would call assassination?” Now, we worked our way around it by little kind of legal sleight-of-hand. We said, “But what if the whole world is a battlefield?” You’re like, “Yeah, you can conceptualize it that way, but that means that other people are going to make the same case and say they can then do things that would once be limited to war anywhere else. Do you really want that is the precedent? You’re like, “Oh, yeah. Yeah.” That’s kind of a problem of where we've moved into this.

There's another issue that I think is interesting related robotics, which is not just in terms of war, but rules at home. When it comes to law enforcement and policing, many of the issues are left — They’re not handle at the federal level, things like police training, use of force questions. They’re not even handled at the state level. They happen at the local level, and the result of that is that we've seen this wide variance in police departments and how they handle really tough questions. Maybe a way of putting it more directly is that you see really good, well-trained police departments when it comes to questions in terms of the use of force, and then you have like the Ferguson's, where they clearly operate in a way that’s suboptimal. They have poisonous relationships with their local citizens. Again, it's not about all police. You have this variance in it and it's everything from the history of those police departments to the kind of training that they get.

We’re about to take that same problem and put robots and maybe even armed robots into that and you go, “Whoa! It sounds like this guy is talking science fiction.” Guess what? Last summer we saw the first police department use an armed robot to kill someone, Dallas Police Department. Now they handled it in a way that you and I could have an argument back and forth as to whether it was done in the way that it should, but it’s a legitimate argument to have, but am I confident that the Ferguson Police Department is going to handle armed robots well? I don't think so. So that's what I'm getting at, is this idea of using a technology and setting precedents for it. It's not just about issues in war. It's starting to move into our own civilian lives.

[0:49:35.1] JM: We had an entire show about the idea of attribution, and I think the ideas of precedent and attribution are closely tied, because if somebody commits an act of violence via drone, for example, and you can't track who's drone that was, then it doesn't even matter who is setting a precedent, because we can't track who they are. Some anonymous drone killed somebody and we don't know who it was. Well, we can't blame it on China or Russia or terrorist or anybody, because it's just an anonymous drone. That's a very scary idea. The guest I had on the show, he was from the RAND Corporation. That was a really good episode, but he was advocating for a type of international Geneva Convention style organization that would help set rules around cyber attribution. Does that sound like a plausible idea to you?

[0:50:36.2] PWS: I don't think we're going to get an entire new set of laws any time soon basically because of the politics of the day. You kind of pull back and you go, "Okay. That might be a really great idea, but would the governments of the world agree to it? And right now the answer is no, and it's both the powers like a Russia or a China that have objected to this kind of approach.

To give you recent examples in both areas that you hit, we've spent roughly the last 15 years building up in the UN the idea that cyber conflict should be shaped by the traditional laws of war and everyone thought, "Okay. Finally, all the different nations the world are on board," and then the Chinese pulled the plug on it.

To the story of robotics, armed robotics is a topic of debate, and there was exploration of could there be some kind of new treaty to potentially ban it, and Russia just came out and said, "Nope. Not to be on board. No global treaty." Just literally a couple of weeks ago from when you and I are talking. You've got that, and then you have the US side of things where for most of our history, we were a nation that pushed for and supported international law, because we saw it as an inherent good. We saw it as a way of protecting our troops as protecting international peace, and now we've got a president who basically takes the opposite to where the United States is operated in its history. So I don't see the Trump administration pushing anytime soon for international laws a solution to, well, pretty much anything.

I see it as less likely to happen. It doesn't mean there isn't a need for it. It’s just the politics of it are unlikely to happen. What you're getting at also with this story of attribution is sometimes there’s a problem of figuring out who did this thing to me, be it a cyber-attack or be it a use of drones or whatever, but there's also — I think we undervalue the — Even if I know what I do about it problem. That's really the problem that we see right now related to Russia and cyber-attacks and the influence operations that you hit earlier. There is no real debate that Russia wasn’t behind. I mean it's the conclusion of the entire US intelligence community, the FBI, at least five different allied intelligence agencies. By my count, also five different private cybersecurity companies, which is important, because private companies in the space, they're prone to disagree. They’re actually incentivized to disagree, to debunk each other's work in the fact that five of them are all agreeing, it adds more validity to it. So you have this widespread of documentation the Russians were behind it.

Now granted Vladimir Putin, but thanks The question is not that, it's, “Okay. What do you do about it?” and the complexity of what do you do about it when it gets fed into partisan politics inside the United States? It's similar to the Sony hack. There was now much doubt that North Korea was behind it. The real problem is what do you do about North Korea, not just in cyber issues, but anything?

[0:54:01.3] JM: When you hear politicians talk about “Russian hacking”, they’re often conflating two things. So there's actual hacking where information is stolen from private servers, and then there's information warfare, like paying for ads on Facebook. What do we actually know about the lower level systematic — What did they actually hack? What was hacked?

[0:54:24.2] PWS: So you’ve hit it exactly right. You have to — On the Russian side, essentially what you're doing is you're talking about the activities of actors, and they've been known as APT28 or cozy bear, fancy bear, basically efforts to break into to hack networks and steal information, versus as you've hit it, efforts at disinformation and influence operations. That’s hubbed out of a group in Russia, for example, known as the Internet Research Agency or they’re also sometimes called troll factories. A way of splitting the two is it’s a difference between stealing information and spreading information even though it's false information.

So the first type of activity, we have seen the targets ranged, and it's important, again, to not put this through the stupid explanations in partisanship that we've seen play out. It was both Republican and Democrat organizations and individuals in the United States both the Democratic National Committee and the Republican National Committee, prominent Democrats John Podesta, prominent Republicans like Colin Powell. We sometimes miss this. We forget it, because it's not convenient to realize that it was bipartisan in the targeting.

It's not just political organizations. It's governmental. The Pentagon joint staff email system, its nonpolitical, nongovernmental American universities, American think tanks, private corporations, we sell banks, nuclear power plants, not just American, American allies. Again, political French election, German parliament, to ones that are government agencies clearly military, Danish Defense Ministry. Ones that are kind of military, but also not, the Norwegian Nuclear Institute, elections in Hungary, Brittain, you name it. International agency, the world anti-doping agency soon after non-coincidently Russian athletes were caught doping. That's all the kind of hacking, stealing information targets. That's different than as you put it, the information spread, disinformation spread, influence operations side, which we saw the scale in terms of tens of thousands of fake accounts that are posing as everything from American veterans to political. My favorite was someone who posed as a young American woman who was pop culture savvy, but also tweeting out on Trump. Political organizations. One of the most influential post is if it was the Tennessee GOP turned out to be a Russian troll factory. Again, spreading misinformation, disinformation, related but different from stealing information both played. Arguably, the second was more impactful.

[0:57:34.3] JM: Right, and all of that is scary, but do we know about voting machines? Do we have any idea if voting machines were hacked?

[0:57:42.9] PWS: There is a back-and-forth on — What do know publicly is that the broader voting system was, in terms of certain at the state and county level registries and the like, there's been enough documentation of that. There has not been in terms of voting machine, changing votes. Again, I'm not saying it did or didn't, I'm saying in terms of the documentation I don't think you can make that case as supposed to you definitely reported not just by media, but FBI and alike of going after broader voting systems.

Again, was it as impactful as going after the broader election that is targeting not the voting machine, but the voter’s mind? That clearly happened and it creates the wonderful what if that wouldn't be solved without a time machine, which we’re going through in the United States of, “Gosh! An incredibly close election decided by 77,000 votes. What if the government had done something more about this Russian activity? What if the social media companies had done something about this level of activity before rather than after the election? What if Mitch McConnell when there was a point in time that there was supposed to be a bipartisan push back against this Russian activity?” This was in the summer of 2016 where the idea was that political leaders from both Republican and the Democratic side will come together and say, “We disagree in our politics, but we agree that a foreign government should not be interfering in our election,” and Mitch McConnell refused to do so. These are what-ifs that were playing out in America, the same kind of what if is happening in in Great Britain where you Brexit was a close — Not as close as the 2016 election in the US, but it was relatively close. Then now as they peel back and go, “Wow! There was this massive level of Russian fueled social media. Was it enough to have influenced the vote?” You can’t answer that, but what we do know is people's activities have been influenced and what to buy and what to believe and who to date in these spaces. Are we trying to say that it doesn't affect — The one space it doesn't affect is your politics. In fact, we know that's not true. We know that the companies realize it, because simultaneous to when, for example, a Zuckerberg was giving that, “Well, it's pretty crazy that people be influenced.” The company was actually marketing to political campaigns, saying, “Social media is the best place to influence voters.”

[1:00:33.9] JM: I was at a conference a few weeks ago, Q-Con, it’s a conference for developers, and one of the keynotes was about — It was an engineer who had worked at Twitter and he was talking about some of the regrets that he had. He was like, “When I think back to it on my time at Twitter, what do I feel? Well, I feel honestly a sense of regret,” because essentially the platform — The way this platfor is developed is they are biased towards generating more traffic, which generates more advertising revenue and they incentivize salacious behavior, and so this is what allows this kind of, if you want to call it, hacking. This information warfare to be so profligate, because the platform is basically incentivized it. Not only does Russia want to hack it. The platform is basically built to encourage it.

I think this relates to the idea that you've touched on where military tools — First of all, this is a military tool, like it is being used for warfare. Social media is being used for warfare. It might as well be a military tool. We have military tools which are much more in directly artificial intelligence related, like if you have a heads up display that's looking for enemies and then you have to have a machine learning algorithm that detects what is an enemy or is this 99% an enemy 70% an enemy. You've got drones that are flying overhead and they're making that same kind of calculation. It's just underscoring — First of all, like AI/machine learning. These things are not really like totally opaque. These are algorithms that engineers develop and they make subjective decisions when they're developing them, and the way that they evaluate the subjective decisions is with their judgment. It is very important for software engineers to have good judgment today.

So my question to you is what advice do you have for engineers in the audience who are listening and they're trying to develop an appropriate framework to vet those decisions of judgment?

[1:02:40.2] PWS: Gosh! You hit so much there. The first is there is a history to this that each generation we and try and forget our claim that we're the exception to it. Creating a certain kind of technology and either believing that it will somehow cure all the world's ills or that one has no responsibility or bearing for how it's deployed, how it's used. If we're talking about a technology like social media, the parallel of the gentleman that you mentioned, you can go back in history and the telegraph was — The creators and the early users of it described how it would bind the world together and how there would be no more wars. It would be a means of creating peace, and my favorite illustration of that was that the very first message sent across the transatlantic cable was that. It was the idea that this, finally we've got this connection, and there will be peace. Then one week later, the telegraph was being used to communicate military orders.

The same phenomena of social media, as you hit it, it's been a platform that has been used to connect us, to bring us together and share the silliest of jokes. It's also been used as a weapon and it is a battlefield. In some cases, even those jokes have been deployed as weapons. When you think about how it's been — Things that have played out in our politics, you name it.

There's this idea that it's only going to be for the good and instead, yes, it's a technology. It can be used for both good and bad. I think particularly relevant to company responsibilities, individual engineer responsibilities, is to recognize a couple of things. The first is in many of these areas, people believe that they're creating a technology, a product, but what they're doing is creating a platform that is in many cases they do not believe themselves to be at a media company or the equivalent of an infrastructure company when they really are. They see themselves as tech companies as supposed to media companies, and you can see this in the challenges that social media companies like Twitter, Facebook, you name it, have gone through where they're like, "No. No. No. We're just a tech company." You're like, "No. No. No. You've become the modern version of a media company. Like it or not, you've become the equivalent of —" Someone once famously told Zuckerberg, "You're the most powerful editor in history." Now you can choose not to use your editing power, but that's your choice. You are in this role, like it or not.

There's another part of this of the way they've done beta testing where they will throw products capability. They will throw things out into the world and then go, "Yeah! We're just going to learn from it, and then later on we'll come back and fix it," and you can see how that's played out in certain areas where you've seen actors manipulate and weaponize it. The example of the algorithms that drive the newsfeed where it could've easily been predicted that bad people would try and manipulate that system and only now are we starting to develop the countermeasures to it.

So what we're talking about is the need for companies to do something that militaries do, which is to read team, that is don't wait for the actual battle, don't wait for the bad guys to get their hands on your stuff. Game it out, play it out beforehand, use training lab equivalents, exercises, bring in people to go after it. Again, some people in the software programmer side will go, "Oh! You mean they can kind of like pen testing in terms of like trying to find vulnerability before the bad guy does?" But it's not just about finding holes in the network to our larger conversation. It's about trying to figure out how might they use your product in a bad way even if it doesn't have any vulnerabilities in it. Think about like how a criminal, how an actor like a Russia might use or misuse their system. Don't wait for it to happen. Don't just throw it out there in the world and say, "I wash my hands of it. I'm just a tech company."

[1:07:08.4] JM: P.W. Singer. Thank you for coming on Software Engineering Daily.

[1:07:10.9] PWS: All right. Thanks for having me.

[END OF INTERVIEW]

[1:07:13.4] JM: Who do you use for log management? I want to tell you about Scalyr, the first purpose- built log management tool on the market. Most tools on the market utilize text indexing search, and this is great for indexing a book, for example. But if you want to search logs at scale fast, it breaks down. Scalyr built their own database from scratch and the system is fast. Most of the searches take less than a second. In fact 99% of the queries execute in less than a second. That's why companies like OkCupid Giffy and CareerBuilder use Scalyr to build their log management systems.

You can try it today free for 90 days if you go to the promo URL, which is softwareengineeringdaily.com/scalyr, S-C-A-L-Y-R. That softwareengineeringdaily.com/scalyr.

Scalyr was built by one of the founders of Writely, which is the company that became Google Docs, and if you know anything about Google Docs' history, it was quite transformational when the product came out. This was a consumer grade UI product that solved many distributed systems problems and had great scalability, which is why it turned into Google Docs. The founder of Writely is now turning his focus to log management, and it has the consumer grade UI. It has the scalability that you would expect from somebody who built Google Docs.

You can use Scalyr to monitor key metrics. You can use it to trigger alerts, it's got integration with PagerDuty and it's really easy to use. It's really lightning fast, and you can get a free 90-day trial by signing up at softwareengineeringdailycom/S-C-A-L-Y-R, softwareengineeringdaily.com/scalyr, and I really recommend trying out.

I've heard from multiple companies on the show that they use Scalyr and it's been a real differentiator for them. So check out Scalyr, and thanks to Scalyr for being a new sponsor of Software Engineering Daily.

[END]