The Future of Irregular Warfare

August, 2020 • 51:49

SUMMARY KEYWORDS

Irregular Warfare, artificial intelligence, technology, information

SPEAKERS

August Cole, P. W. Singer, Nick Lopez, Shawna Sinnot

Shawna Sinnot 00:00
Hello, everyone. Thank you for joining us today on the Irregular Warfare Podcast. I'm Shawna Sinnot, one of your co-hosts. And before we start today's conversation with P. W. Singer and August Cole, I wanted to let you know that we're currently searching for a fourth co-host to join our team. If you're interested, please send an email with your resume to engage@irregularwarfarepodcast.com. That's E N G A G E @irregularwarfarepodcast.com. We will accept applications through September 15th, 2020. There are no hard requirements, you can be civilian or military, a researcher, policymaker or practitioner. The key criteria is just that you have a deep interest in learning and sharing knowledge about irregular warfare topics. So thanks for listening and enjoy the conversation.

P. W. Singer 00:52
Overall US cybersecurity strategy, a document that came out roughly the same period that the NDS did, you know how many sentences it has on the weaponization of information? Zero.

August Cole 01:06
The strategic Corporal is once again a relevant concept because of the Twitter account.

P. W. Singer 01:13
To put a fine point and I think there's in particular, two draw lessons that "Burn-In" has for the community working on irregular warfare issues. One is about the whole suite of technologies that will be available to them. But then the second is the change in the operating environment driven by this industrial revolution.

Nick Lopez 01:40
Welcome to episode eight of the Irregular Warfare Podcast. Your hosts today are myself Nick Lopez, and my co-host Shawna Sinnot. In today's episode, we take a look at the future of irregular warfare, its implications on defense planning, policymaking, and what the future irregular warfare practitioner will look like.

Shawna Sinnot 01:57
We talked with two bestselling authors who have conducted extensive research on how technology will drastically affect society, the economy, and all things defense related, especially in the realm of irregular warfare. They take this research and weave it into thrilling stories that portray the future of conflict to include the best seller "Ghost Fleet, A Novel of the Next World War" and their recently released "Burn-In: A Novel of the Real Robotic Revolution". Their books are on military and government professional reading lists around the world.

Nick Lopez 02:25
P.W. Singer is strategist at New America and a professor of practice at Arizona State University. No other author has more books on professional military reading lists. He has been described in the Wall Street Journal as the premier futurist in a national security environment. He has been named by the Smithsonian as one of the nation's 100 leading innovators and by Foreign Policy to their top 100 global thinkers list. You are listening to the Irregular Warfare Podcast, a joint production of the Princeton Empirical Studies of Conflict Project and the Modern War Institute at West Point, dedicated to bridging the gap between scholars and practitioners to support the community of irregular warfare professionals. Here's our conversation with P.W. Singer and August Cole. P. W Singer and August Cole I know I can speak for the, for the team here by saying we really enjoy your work with "Ghost Fleet" and your most recent book "Burn-In". So with that, it's great to welcome you both to the Irregular Warfare Podcast.

Shawna Sinnot 02:48
August Cole is a non-resident Fellow at the Brute Krulak Center for Innovation and Creativity at Marine Corps University, and a non-resident senior fellow at the Brent Scowcroft Center on Strategy and Security at the Atlantic Council, where he directed the Council's Art of the Future Project. He consults on creative futures at SparkCognition and is a regular speaker to private sector, academic, and US and allied government audiences. He is also the author of numerous short stories about the future of conflict.

P. W. Singer 03:48
Thanks for having us.

August Cole 03:49
It's great to be here.

Nick Lopez 03:49
All right, I'd like to jump right in by talking about your most recent work "Burn-In," we'll start with Peter, what was the motivation behind the work and how did you all get started?

P. W. Singer 04:00
Sure. So "Burn-In" is both a continuation of something we tested out with "Ghost Fleet" but also taking it into both new topics and new levels. So "Burn-In", it's a smash-up of a novel and nonfiction. Now that sounds kind of odd to say it that way, but what it is, is it's a techno thriller. You follow the hunt for a terrorist through a future Washington DC. And so of course, you know, that's fiction, it hasn't yet happened. But baked into the story are over 300 real world explanations and predictions of everything

from okay, I keep hearing about AI; how does it actually work? To what's the next Special Forces sniper rifle going to be like? To dilemma questions that will emerge from new technologies, information overload issues, new ethical issues like algorithmic bias, all of these different sorts of questions and issues, there's 300 of them baked into the story. And there's actually 27 pages of research in notes to document, hey, that's not what Peter and August dreamed up, that's actually, here's the study that backs it. Or, here's the contract announcement order for that sniper rifle. Or here's a white paper, if you want to learn more about this topic that we just experienced in a scene. "Ghost Fleet" explored what a future war, particularly a great power conflict might look like. "Burn-In", in particular tackles what we think is one of the most important if not the most important technology, but also social, political, economic, moral, legal security, when you think of its impact, issue that's out there, that's in turn, arguably the least understood. Which is you know, what's going on with AI, automation, Internet of Things, these massive changes to our economy, but also to war, you name it. And so we use the fiction to explain that.

Shawna Sinnot 06:04
Yeah. And that's a, it's a really unique vehicle to be able to convey imagination, which I think some of us who are in more, you know, linear professions struggle to do. And so the way that that looks at the future is very interesting. August, could you tell us what FICINT actually is, and about how to use this framework to explore the content that Peter just explained?

August Cole 06:25
When you look at the different types of fiction writing out there, particularly science fiction that can be useful to professional military leaders in that community, it's important, I think, at the same time, to really start to unpack what is and what makes those things actually useful in those kinds of stories. So the FICINT framework was something that kind of began somewhat tongue in cheek in using it because I was trying to think of a way that we could discuss the sorts of books like "Ghost Fleet", the sorts of short stories that you might see on the army mad scientist blog, that are trying to address big policy questions, real world implications of technologies that are, you know, almost existential. And it's a mash up of the idea of fiction plus intelligence, the same way you might have, like, human intelligence, it's human. And, you know, when people started to hear that, you know, nobody laughed, like, which is obviously a good first order test, when you're talking about this in a presentation, you know, something Pete and I really started to hone in on is almost like rules for FICINT, from starting is kind of a larger sort of notional idea of what it is, to having a much more, much more clarity. And so that could be you know, being able to you know, huge rules that for example, represent technology, not as people want it to be but as it is, or you know, to take the Fog of War construct from Clausewitz, like that's going to be there in the future too. And all the salesmanship, if you will, and aspirational aspects of technology, which are of course, important to realizing their potential, you know, that can also be analytically very dangerous, because it can allow us to place too much faith in certain systems, in particular if adversaries are already you know, queuing to exploiting that overconfidence potentially. So, you know, the other facets too, I think you can see in FICINT, that are manifest in "Ghost Fleet," that are manifest in "Burn-In," are things like endnotes, allowing at least enough tethering to economic, political, technological trends so that a reader just doesn't go "this is crazy."

Shawna Sinnot 08:19
And that's what Nick and I were talking about this and I think that's what stood out the most to us is every detail, if it was something that we knew, and if it was something we didn't know, it sounded legit.

Nick Lopez 08:26
Yeah, I'll second that, very well detailed. So one of the things I'm interested in is how your research shaped your approach to thinking about some tools that AI affords like the weaponization of information.

P. W. Singer 08:39
Absolutely core issue, but we need to divide it out in a couple of ways: on the weaponization of information side, and in particular, we're talking about, you know, what, in a prior book I called "Like War". So if you think of cyber war, it's the hacking of networks, stealing information, embed intellectual property, be it your credit card, "Like War" is not about hacking the network, but rather people on the network driving ideas viral. And again here it might be driving terrorist propaganda viral, it might be driving election misinformation, or even Coronavirus misinformation viral. Just like in cyber conflict, the goal is not the network activity, it's the real world, it's have a real world effect. So it's to you know, in "Like War" we began with a look at the Battle of Mosul and how what played out on social media actually affected literally, the outcome of that battle: Iraqi units dissolving, or it's having an effect on people's beliefs, what they vote on, it's to have an effect on what products they buy, you name it. And I think it's interesting because it is a crucial part of what drove us to rethink on great power conflict as a priority. And yet we still don't get it right. And by that, I mean, we've added Russia as a, you know, greater competitor in the National Defense Strategy. But Russia didn't become a greater competitor because it's single aircraft carrier that's dated and actually caught fire and sank in drydock. They didn't become a greater competitor because they got more, thousands of new tanks. They became more of a challenge because of this part: because of, that's where their power has come from. And yet, think about what we've done to counter it. Overall US cybersecurity strategy, a document that came out roughly the same period that the NDS did, you know how many sentences it has on the weaponization of information? Zero, your quick answer is zero. You've got a lot of stuff on protecting critical infrastructure got nada on this space. I mean, we have different things going on, you've got a little element going on in NSA, you've got people in public affairs learning more, but in terms of State Department, or how we've changed the education system, how we're, right now, not handling/mishandling ongoing information threats to our election, we do not have a national strategy for it. And we can unpack a lot of reasons for it. But it's a major gap.

Shawna Sinnot 11:16
Well, Peter, you mentioned Russia in their weaponization of information. But what does this look like with a more capable adversary like China, who might use this in conjunction with automation and artificial intelligence?

P. W. Singer 11:27
What we look at in "Burn-In" is, it's not the classic framing of an arms race of who gets AI first or whose AI shoots further if you think about, you know, the arms race with the Soviets. Instead, it is an arms race in a certain way, but it's about two totally different competing visions and applications of AI in

terms of an industrial revolution. You have, you know, the Chinese model, which is massive, and AI, we're not just talking about AI itself, but broader automation, unmanned systems. But it's not just in the military side, it's on the society wide side. And China has a plan to be a world leader in AI and automation technology by the year 2030. They've got a strategy to back it. But it's a very centralized approach. They've chosen their national company champions, and all data has to be shared with government. By contrast, in the US, we'll see just as much automation AI happening. It's just kind of spread out, you've got Google changing it, you've got Facebook, you've got, Kentucky Fried Chicken had a face recognition program, you've got the US Military has a cacophony of AI and automation programs. And so there's two very different visions. But the better way to understand it, like we try and explore in "Burn-In" is understand it's an industrial revolution. It's not about one single type of robot or one, HAL 9000 superintelligence. It's more about what played out with steam engines or another example would be electricity.

Shawna Sinnot 13:11
So when we think about how conflict might look with this type of weaponization of information, August, can you speak to how this might look different from a conventional war that we might used to, to in irregular warfare contexts, which might be a more likely scenario when competing with our peers or near peers?

August Cole 13:26
I think that's a great follow up to what Pete was just talking about, in part because the synergy of AI and our National Defense Strategy, you know, if we are reorienting in the US towards China, and to a lesser extent Russia, as this sort of near-peer peer, you know, framework and what we're not, I think, appreciating within that is, yes, technologies like AI can be, you know, capital level national priorities, with, you know, in China's case defined very big budgets that dwarf ours. But we're also I think, not looking at the second and third order effects of that industrial revolution aspect to AI that Pete talked about, and that to be putting forth a strategy that doesn't acknowledge the vulnerabilities at a systemic level in the US. So if you're going to think about being at a deterrent posture, in the 2020s, and into the 2030s, because I really do believe between like where we are today, and where we are in the late 2030s is probably the most critical like 20 years of this, of this century, that what will happen with China's ascent, and the technological breakthroughs and capabilities like AI and autonomy are going to, I think, very much determine the next 60 years that follow. So if we, if we look at America in 2025, right, you know, five years from now, and our social contract is weakened, we have far more technology, remote work, we have far more 1099 Gig work, we're going to have essentially transformed in many ways that policy won't have caught up with and the country may be more vulnerable at a social and political level. That is not the place I would want to be when, when conducting a great power strategy and executing in a way that looks like you know, you can win that over, over 10 to 15 years, and to root it back into the question of irregular warfare. So, you know, by enabling a society to experiment and of course, adopt and invest in a very unstructured way, that can be very effective and can produce some really high-flying companies and really, really great use cases. But you can't also ignore the gaps and, you know, flaws that that can either create or highlight, that technologies like AI can exploit an information domain, and to see the domestic influence operations around COVID that are being conducted by foreign adversaries just reading about it in the media, it's pretty, I think, striking. And I think an indicator that there is a lot of lessons learned being passed from one nation to another

that you'll see continue and continue and continue. And as non-state actors start to adopt that, I think you'll find a lot more really interesting conflicts taking place. And by interesting, I mean, difficult for the US to engage in in a way that maybe fits into our conventional military models, even if we are, you know, the Special Operations community trying to reframe back towards great power conflict. But does that mean that we turn our back on the experience last 20 years, or there are discrete lessons learned, especially around like cyber information operations, you know, high speed targeting and mission execution. You know, that is going to have to get wrapped into of course, this larger narrative about the enabling power of AI, the rising challenge of a country like China, not just in its backyard, but through Belt and Road or, or potentially on our own soil in terms of influence ops. And then of course, you know, are we really on a solid foundation, to be able to wage that kind of a strategic campaign? And I in all three of those counts, I have a lot of worry.

P. W. Singer 16:32
And to put a fine point and I think there's in particular, two draw lessons that "Burn-In" has for the community working on irregular warfare issues. One is about the, the whole suite of technologies that will be available to them, you know, whether it's augmented reality to AI decision aid systems and the like, and that those technologies will offer new possibilities, but they'll also offer up incredible new dilemmas that will have to be figured out everywhere from tactic to doctrine. But then the second is the change in the operating environment driven by this industrial revolution. And that, both is going to affect the economy, society, politics in the US, but also a wide variety of nations that people might deploy into. To put it bluntly, the last industrial revolution changed much of the world and drove again, you know, everything from how people lived and worked, to how they fought, to even what they fought about. And that's the same phenomena that we're entering into. So I think those are the two particular draw out lessons, but woven in a way that is not here's your 180 page, white paper that you have to read, or here's my stock, my PowerPoint brief on it. Instead, you know, going back to this concept of useful fiction, put into a framework where hopefully, you're simultaneously being educated, but also engaged and entertained. And you know, for some people, it's just going to be a fun read. For other people. It's, oh, that's a little useful tidbit for me.

August Cole 18:18
I might add to that, at the core of a book, like "Burn-In", and we specifically thought about this every single day we were working on it and continue to, is the relationship between a human and a machine and the relationship that that human has with other people and how it's affected by that relationship with that machine. And that is a core facet of our experience as individuals and collectively, we're going to have to start to really wrestle with. There's profound implications in the military domain and the security domain, whether it's the you know, standing army construct, as that starts to shift over the next 15 years because of larger fiscal pressures, the increasing capabilities of systems, and yet to not be too overly, I think, optimistic about the transformational capabilities of software driven platforms, whether they're walking, whether they're handheld, or whether they fly. The thing to always remember, I think, is that we are going to be ultimately in this kind of human context, and that we may have more autonomy and even less human in or on the loop. But the overall arching campaign objectives, especially in irregular warfare, since heretofore had been very human focused. And that's not to say there won't be significant shifts. You know, the primacy of data is of course tied to you know, the relationship you have with that machine. You know, in "Burn-In" Special Agent Lara Keegan has this, this TAMS-the Tactical

Autonomous Mobility System, which is kind of like an earmark type robot that she's been assigned to work with effectively by the Justice Department as an FBI agent. And she's essentially seeing that relationship change the more and more data the robot has access to. And that's, I think, a really important paradigm you don't often see in narratives about machines but reflects the reality. It reduces both trust, but also confidence as well in being able to rely on that system. And her background as a robot wrangler in the Marine Corps, I think gives her some initial skepticism and kind of a realistic way of looking at the technology that I think helps the story, you know, kind of start, but also, I think gives you a fairly accurate way of how people who are in professional military might actually relate to machines throughout the course of a campaign, an operation, or a career.

Nick Lopez 20:25
So Special Operations Command invests a lot in human capability. And there's five Special Operations truths. The first is that humans are more important than hardware. In "Burn-In" the protagonist, Special Agent Lara Keegan, was initially assigned the robot and she was apprehensive. However, she received a lot of pressure from within the FBI to go through the process of utilizing the robot and the technology. So I'm interested, from your perspective, what's needed to onboard technology at scale, while still maintaining the importance of human capability?

August Cole 21:09
I think we can have a lot of maxims, right, about let's say that, you know, the Special Operations community and, and some of those I think, are enduring, and some of them are going to be changing. Right. You know, I think the things that are going to be consistent are, of course, as you said, the importance of the individual, the value, and training, and experience, and maturity. I think the question and the challenge, though, as you've seen the need for the US Special Operations community scale up dramatically more probably than it would have naturally done, you know, outside of the 9/11 framework, and, you know, being able to give people you know, those three qualities, going into the future. And again, if we're going to, by extension, say this is a Special Operations community that's going to be very active in this great power campaign globally. You may need even more people than you have today. And so the question, I think, becomes one, do you try to keep growing organization? Or do you try to take those traits and qualities and spread them throughout the general purpose or regular forces? And certainly there are systems that are, you know, AI based software, you know, whether it's guidance, whether it's, you know, the sorts of analytics that can be used real time by individuals, I think, almost force an existential question upon the Special Operations community, right? Do you spread this off, you know, more? Or do you reduce down to have a fewer and fewer number of people who invest more and more technology, because government does not have a track record of spending more and more on capability, and necessarily getting what it wants out of it? You know, the, not that people are becoming aircraft platforms. But you know, you can look at the paradigm in that world too. So you know, if if SOCOM in 2040 has 300 people total, it may be yes, they are super enabled, the equivalent of an F-22. But that's probably still going to be out of step with the reality of operations around the world and the missions that are, that it's called upon to do that. At the same time, I think that a lot of the capabilities to shape the environment and to understand it, importantly, are going to be really interesting to see those move off of platforms, right. And that's going to be requiring individuals to have new interfaces and interaction with that kind of information and data. So you know, to be able to in an entirely tactical sense, understand what's going on from around you, not with that Minority Report style, augmented

reality glasses construct, which is really cool. But I've been thinking a lot about actually the haptic aspects of situational awareness and the ability to be able to deal with the cognitive overload that we talked about in "Burn-In" is a real problem. And in the law enforcement and counterterrorism context, that's only going to increase as we get more and more access to data. So you're gonna require machines to make decisions not so much about what the target is, but about what information you should be looking at. And then I think we're trying to kind of, from what I see, you know, make sense of which technologies actually can shape that future. Talking about technologies shaping the future, I can't help but think about companies like Neuralink, who are attempting to integrate or fuse human and tech directly. Right. So one of the things that comes to mind is brain machine interfaces. So August, I'm interested in how you see BMI or brain machine interfaces, affecting the future of irregular warfare. I think the, really science fiction advances that, that really do fuse human machine at that neurological level, are coming and probably going to come out of the commercial marketplace. First, I'd expect gaming will be one of the first places you see that emerge, I think medicine too, imagine like doing Robo surgery with that kind of a neural link capability would be really interesting. And you know, the military is probably going to lag. And there's gonna be adversaries and small states or small groups rather, that aren't going to be wed to convention ethics, norms, you know, budgetary cycles and priorities that allow them to be more experimental. I mean, this is a really interesting challenge. And again, in the irregular, unconventional warfare construct, like if there's US allies, that we partner with, is it possible that we can see them actually being more experimental say in the Indo-Pacific? With some of these technologies, where we are working with an allied nation and their, you know, pure Special Operations community may actually be more forward in this than we are, because of, again, an imperative that is going to become, I think, increasingly real, which is, you know, how do you create deterrence and capability in the shadow of China. But also because the, the paradigms are breaking down on the defense industrial side, and there's less and less, you know, obviously, political value plays to those deals, you know, currently with this administration. And we'll have to see with the next one. So I think you're going to be freeing people up to kind of re-baseline bilateral relationships. mil-mil relationships, not just on hey, did you buy the same like, you know, hardware that I did that came off the same line in the same state in America? Or rather, you know, are we really aligned strategically and operationally and you know, are there other technological capabilities that then we can arbitrage to and say, hey, if there's a partner nation that has this capability, we want to use it. And I think actually, from a US SOF point of view, I would probably be encouraging that. Because there may be ways that you can start to leverage and really reframe that when we engage in a partner capability in a, you know, for internal defense context, like, do we have to be the most sophisticated technologically in that context? Or can we have better awareness and kind of, you know, almost an anthropological sense of feeling for what's going on, and truly allowing other people to do what they need to do. And being the best enablers that you can. That's a very different context than coming in and being the quietest, the stealthiest, the most effective. But it may be something that is a kind of a new iteration, because of that technological democratization. That doesn't necessarily mean that you know, a Green Beret team is going to have the best comms, the best brain machine interface or, you know, even on the social media side, the best ability to you know, conduct Like War like Pete said.

Shawna Sinnot 26:45
Yeah, and I think what's interesting about these technologies is our inclination is to think of them in an offensive context, when we're talking about acquiring them and employing them. But what, you've

alluded to some of the challenges, "Burn-In" really emphasizes the susceptibility to exploitation. And it's in that, that domestic context there, but can you speak to what that looks like and what we might be missing in terms of both friendly and adversary exploitation of these technologies?

P. W. Singer 27:11
So I think there's a couple of things to think about in terms of that, one that we've already hit before, is the idea of influence operations taking on a whole new level. What you have playing out with the change to what we call the Internet of Things, is that you've got, you know, this wide variety of platforms out there that have sensors, so think face recognition, which has been, you know, whether it's, there's a DoD program, to do face recognition at 1000-meter distance in the dark. But you also have, you know, everyone from police departments, to companies, you know, Rite Aid, actually was just revealed to have been quietly running a face recognition program of its customers. So that allows you, okay, this is the person's faces, and to match it to an identity. That's Peter, who just walked in. But then I can take that data, and connect it back to everything that we've been able to gather about Peter, and even more so people like Peter, everything that's been posted, everything that's been bought, et cetera. But importantly, not just do the history, but move forward. This is what's Peter as an individual, or someone's having these attributes might do next. And here again, you can think about that for marketing purposes, political purposes, targeting purposes, figuring out military moves. But to influence, not just predict, but influence. So we've got all that going on. And it will be done in ways that are overt in ways that will be covert and not well understood in the background. And it'll happen, we'll have tactical application, we'll have strategic application. So that's one issue. But the other is, unfortunately, we are baking into the Internet of Things, all the mistakes that we did with the first couple generations of the internet. So you also now allow cyber-attacks that will have kinetic impact. And here again, it might be something at a very tactical level. So not to spoil the book for people. but you could, for example, kill someone in a smart home without ever leaving your home using digital means. The impact of that, of course, is you know, it opens up all sorts of new possibilities for our own operations. But it also means that it can be done against us. And again, whether it's against military targets, you think about the emergent smart bases, to the wider civilian system.

Shawna Sinnot 29:45
Yeah, it's interesting. To August, when we think about the ways that we're protecting that are we, are we doing a good job to make sure we're not becoming vulnerable to a lot of this exploitation? And I think that goes to something you've also talked about and mostly with supply chain risk management and some of the vulnerabilities that are apparent there. But structurally, are we paying attention to this?

August Cole 30:05
I mean, the, you know, the first step is recognizing you have a problem, right? So, you know, we have that conversation happening about some of these vulnerabilities, which is, which is great. The critical thing I think comes down to though, like probably three areas, one is having as many people involved in that debate and dialogue as possible to get truly innovative and unusual solutions. The second is, I think, being able to accept vulnerability, and understand that your ability to persevere through it, you know, resilience is the word that's often used in the Homeland Security community, and in the cyber community, I think it's really apt, especially as more infrastructure begins to, to get wired up, especially things that may not have been intended to be put on the internet. You know, maybe in again, two, three

decades, you may have, you know, new start, you know, systems that are doing bedrock infrastructure. And America is due for, you know, probably a couple of trillion-dollar infrastructure upgrade, you could do that more securely than trying to like, you know, rewire sensors to pass old bridges, water systems, electrical, but I think the last is kind of a cultural question, you know, to understand that, like, you know, the human and cognitive domain is a terrain in which we are being engaged on. And it's not just, you know, kind of a reframing of like, the old, you know, marketing kind of assault that, you know, Madison Avenue, so to speak, you know, has had on us since the 50s. But rather like this is actually, there are strategic, there's strategic intent from, from nation states and from individuals who are often aligned with them. And we have to accept that, that we need to invest more in education and preparation, that allows us to weather that. Because you remember, that even an organized, you know, military, like ours, in a western society, it's an all-volunteer force, we're drawing people from the general population. So the more I think you can prepare people before they serve, the more you can prepare people who are in critical functional roles in society. Again, these are not like really complex or really difficult policy, I think ideas to execute, it really comes down to, again, rethinking education, rethinking investment in the social contract.

Nick Lopez 32:04
So it seems like the proliferation of this technology lowers the barrier to entry is what I'm understanding. So I imagine you'll think that non state actors will utilize this to the greatest extent possible, making irregular warfare practitioners with Lara Keegan-like traits, all the more important moving forward. So what does the ideal future irregular warfare practitioner look like?

Shawna Sinnot 32:32
Other than being a great female protagonist, which is awesome.

P. W. Singer 32:34
I'll jump that on two ways. One is, you actually hit that which is, there's stereotypes of who does certain roles and how they look and what their background is. And as we all know, that's not always the best way to find the best talent for it. So that's, that's right at the top, hit that, but in terms of a character, and kind of the skill set that Keegan brings. But one of the things that sort of the attribute that she brings, that I believe is going to have to continue, is this cross between an understanding of the technology, how it works, but also where it doesn't work well? What are its strengths? What are its flaws, and then an ability to kind of always constantly pull back and think about not just what is the technology doing, but the context that it's within? And the effect that it's having both on that context, but also on herself? And, and also trying to figure out why is it operating this way? Is it operating this way because it was programmed to do it? Or is it taking some kind of data and mishandling it? So kind of what I'm, I go back to it's just, it's a facility with technology, but not putting it up on a pedestal and thinking that it's the solution to all your problem sets. It's to be realistic about it. So she understands the advantages of it. There's not, she's not a Luddite, but it's also she's not, you know, one of these Silicon Valley folks saying, yeah, it's gonna solve all our problems. That to me, you know, how do you get that, that's not just a personality issue. There's, there's a training aspect to it as well.

August Cole 34:24
I think there's another aspect too which is being surrounded by technology and having the training and therefore the confidence to make those kinds of calls like Pete said, to be able to say definitively "this system is not doing what it needs to do for me right now, I'm going to ignore it." And that I think, is something that only comes from experience. The good thing is though that you know, a simulation and particularly as it relates to using systems like AI or software like that, we are at an age where we will be able to more rapidly iterate. But I will submit though there is still nothing that will replace real world experience and understanding you know what actual stakes are with a piece of technology when someone's life who's standing next to you would be on the line. To me, that seems like a very critical aspect. And so the way you would, I think, incorporate that into the current force, because the current force is the future force is to begin by, could you give every army recruit or marine recruit in basic training, you know, a drone? A bot? Kind of essentially like in that Tamagotchi way, you know, keep alive through that through that cycle, right? The Marine Corps transformation, pushing small bots down to the squad level and below, I think is a really intelligent way to approach this, because by design, you're going to be therefore expecting young individuals and Americans to break these things, to lose them, to mod them, to race them, to fight them, to do whatever. And that's the point. So to not create that kind of like, oh, you broke it, you're in trouble, accountability around systems that should be attritable in the first place. So there's a position shift to, from everything from the acquisition system to doctrine and tactics that goes with that, but the more you can saturate people in technology, because when they come in, as civilians, they've been growing up with it, like my kids, you know, will have been swiping screens and playing with controllers and flying little drones, you know, pretty much since they could, you know, write their own name. And I think that, to me, speaks to the effect of how far you can see, almost like being out of phase with broader global trends, technological trends, that I'm pretty sure that other parts of the world, just as you've seen, for example, the rise of cell phones 30 years ago, or, you know, over landlines in parts of say Africa, where development was not facilitating the kind of infrastructure that in the West, we would have built or had built over the prior century. You're gonna see those kinds of technological uptick and adoption, experimentation happening at a very young age as well. And in the West, we have to have that same mindset, I think. It's also key to understanding how an adversary is going to operate. I mean, you think about the surprise that ISIS presented to us, much of it was ISIS members acting like, frankly, you know, what other Millennials would do, you know, going back to the discussion, that we have frequently of, you know, ISIS was so good at social media.

Shawna Sinnot 37:02
So is every other 20-year-old.

P. W. Singer 37:03
They were basically doing things that any other teenagers were doing, or ISIS deploying unmanned aerial systems in both surveillance and later on in attack roles. They were basically, you know, Jury rigging ones that were available to almost anyone. So I think, you know, having that facility with technology is also going to be key to understanding not just what are the possibilities for us, but what are the possibilities for adversaries too?

Nick Lopez 37:30
Pete, you mentioned election and Coronavirus misinformation. I want to come back to that as irregular warfare seeks to influence and gain legitimacy amongst populations. As misinformation and disinformation are huge threats, other than education, what are what are some implications that you pulled out of your research on combating misinformation and disinformation?

P. W. Singer 37:54
So like everything else, you first have to admit that you have a problem. And then you build a strategy to deal with that problem. And unfortunately, and this is something that is, it's a differentiator between the states that handle missing disinformation threats, well, like the Estonians of the world, the Canadas, it's the Finland's etc. And those that have, are basically pointed to as being the pits at it, and that is the US followed closely by the UK in terms of democracies. It's, you know, admit that you've, you're handling this bad, and unfortunately, we've there's some partisan political issues that have prevented us and in the UK from coming to grips with that. Okay, so then you build a strategy. Also something that the Estonias etc., have that we don't. That strategy, like any other good strategy should not be based on the hope for a silver bullet solution. One solution? No, you're not going to solve this. It's, it's about risk management. As long as you have the internet, as long as you have people, you're going to have missing disinformation threats. And with AI, they're only going to grow worse. Silver Bullet, there's no one thing that you do, you build up an approach that brings together a wide array of actors. And there's a great parallel to both regular cybersecurity but also public health in this space about what to do about disinformation. And it's basically that you have a role for government, and it's across government, you have a role for the private sector, you have a role for the individual. No one in cybersecurity would say, well, they created Cyber Command, I guess my mom doesn't need a good password on her Gmail. And yet we kind of want that in this space. Right. So government, we need a strategy that sets up a division of labor of who does what. That division of labor plays out everywhere from within the military. And we have a little bit of a battle going on in the military right now. From what, t one point in time, no one was doing it to now you have, you know, everything from Cyber Command says it's ours, Special Operations Command says no, no, no, no, it's PSYOPS', and then Info Ops will go no, no, it's not PSYOPS', it's, it's Info Ops, and Public Affairs is like, whoa, whoa, whoa, what about us? It's in the public. So but it's not just that, figuring out that division of labor. It's literally how are you changing professional military education? Here, again, think about the parallel to cybersecurity. Yes, we created Cyber Command. But we also change the training for every officer who needs to get a little bit of a dose of this. And it's not just about understanding threat environment, it even extends to how do I do this individually. I do talks for the new flag officers in the different services, the new three stars. And, you know, we'll talk about large strategic disinformation threats. But there's also this gap of, no one's ever taught them on how to use their own social media accounts effectively. And so it's, think about the systemic change within the military, not just I'm saying this is the Oregon charge of it, it hits all the way to PME. But you could do all that within the military. And it would not be enough, if you don't have the key changes within the intelligence community prioritizing this kind of threat. Estonia, for example, knows better than anyone, the real threat of Russian tanks rolling over you. And yet they've changed their intelligence system to do a better job of understanding incoming disinformation threats, because they see it as, as just as or in some situations more threatening. So there's so much more that can be done. Are we doing it? Unfortunately, we're still well behind.

August Cole 41:36
You know, I think that there's another side to that question, which is, and this relates to the Special Operations community, and that's how do you utilize those very capabilities overseas against adversaries? And if you are in this era of increasing technological capability, most likely, you know, autonomy, how do you push that capability, and importantly, the permissioning behind it lower and lower into your formations? You know, to my point earlier about training and you know, giving people their Tamagotchi drone or, or, you know, UGV, or whatever. If you can train an individual to responsibly use, you know, a weapon, it seems that you should be able to also simultaneously be spending time to responsibly use social media, especially given as Pete said, the strategic impact, you know, the strategic Corporal is once again a relevant concept because of the Twitter account, right, or the Facebook account or, you know, the VK account. I think that is a cultural shift, though, that, obviously in the SOCOM world deals with a lot of silos, as Pete said, between different commands and who has authorities, who is essentially given a seat at the table. You know, if you're unconventional, or excuse me, if your Information Warfare or PSYOPS, people aren't given a seat at the table with the other commanders, so to speak, at that level, you're never going to have I think that voice to say, you know what, we don't need to own this, but we need to help everyone else propagate this throughout. Because if you're going to be operating in small teams, and not be given those authorities or having lengthy, you know, if we're moving much slower than adversaries going to, then I think you're gonna be in a situation where you're not ever going to be effective. So there's question of trust, but crucially training, and it's certainly within our capabilities to do that. But it requires, I think, a very big cultural shift.

Shawna Sinnot 43:23
August, you mentioned some of the cultural considerations at the institutional level, but this comes down to the individual level as well. So what lessons does "Burn-In" have for practitioners in the irregular warfare community about how to approach the future of conflict?

August Cole 43:36
Yeah, I think one of the abiding lessons in "Burn-In" for the irregular warfare community is that you are going to have to have a much more intimate relationship with the information that describes the environment around you, not just in a current sense, but in a predictive sense. And in the book, it's a robot that's like the physical manifestation of that, which is effectively you know, that human machine interface that is like having a conversation with an oracle of sorts. And that relationship between the Special Agent Lara Keegan, and this robot TAMS deepens, of course, the more and more data it accesses throughout the course of the story. But that's not unlike, I think, the same way that, you know, military operations will be conducted in that human-machine aspect. So it, the more for example, exploitation of adversary servers, of battle networks, etc., is going to of course, deepen that relationship with the information in the environment around you. It's really important to think a lot about how that interface goes. And I think giving people who are on the soldier side, or the operator side, or whatever the language to shape that interface, the you know, the UX, you know, the UI and user experience user interface. I think it's critical rather than being told "this is how it's going to be". And I think that actually could be quite important in determining whether that data is truly effective in skewing, you know, operations toward being bogged down in information in an action, to being able to clearly decide what's important and what and you know when to move in a certain way, and what to do with that information.

So being really cognizant of that very human relationship with technology, but ultimately, that's really about the information that's behind it. You know, we are we're going past the platform era, in describing you know, the Western way of war we are, we are in the software era. And that's true for Information Operations is true for kinetic is true for cyber, you know, it's true for space. And I think that is also a critical realization to that a book like "Burn-In" kind of manifests, you know, in a counterterrorism case, that, in many ways is like the hunt for high value individual, right, and trying to unpack and penetrate different networks using technology, but also the human intelligence factors that I think drive, you know, the realistic and kind of real world ways that those sorts of missions would be done in the next decade.

Nick Lopez 45:48
So I think we have time for one more question. And so we talked about implications for policymakers, and also practitioners, I'm particularly interested in what you both think academia should be focusing on in terms of research within the realm of irregular warfare.

P. W. Singer 46:06
I'd suggest a couple of fronts, and there is a start of some really interesting work on each of these areas. But I think we can go a lot further. The first is, you know, near and dear to my own heart, which is, what is the impact of true technologic change on this space? Not just about direct use, but the ripple effect on the broader context? You know, a different way of thinking about it is, I think of the parallel of where we are with unmanned systems is the equivalent of airplane in the teens or the 1920s. Right, we're just scraping the surface of not just what's possible, but what will be the effect on everywhere from tactics to doctrine to, you know, overall strategic behavior. So I think we need to dig deeper on that, and particularly when we think about what from the civilian side will come over, that's, you know, the non-obvious application. The second is, and you're seeing more work on this, but understanding what is the role of this community in great power conflict? And how does it express itself through not just the what we've gotten used to, which is, you know, the foreign internal defense, helping to, helping a government fight against an insurgency, but how does it express itself on the opposite, where we may be the ones behind the insurgency, which oh, by the way, happened a great deal during the Cold War, and all related to that, we still do not have a good handle on proxy warfare, which is one of the, both in terms of us using, but it being used against us and our allies. And you know, this, I could be talking about proxy warfare, whether it's in the Middle East, whether it's in Ukraine, etc., I don't think we've got a good handle. So those are a couple areas that I think should be priorities for us.

August Cole 48:11
You know, when it comes to what's next, for irregular warfare in Special Operations community, it seems like the academic community could spend a lot of time researching how the military will have access to different forms of data, when they'll get it, what they will be able to do with it. And I think that's something that is both a question of norms as much as is law, particularly when you look at the in-extremis evolution of small raiding units in World War Two, say, the British SPS, the rise of the SAS, you know, the kinds of both bureaucratic but also legal, in international sense rules that were broken to accomplish missions that were in many cases strategic. Not always successful. But the point was that there was a fundamental shift going on in the nature of warfare that the West was conducting. And just as then you had, let's say, you know, the Long-Range Desert Group utilizing jeeps, you know, the future SOF formations in the 2030s will be heavily impacted by their ability to access data, when they're

remotely you know, how many if you're looking at a building in a very dense urban environment, you know, how many times was a toilet flushed in a certain apartment? Did that tell you how many people might actually be in there? After a certain person arrives and leaves, you know, is there a pattern of life change? In the same way that we study, you know, adversary server farm operations for, you know, small variations in temperature or whatever they, you know, the spooky folks do? You know, I think that level of data that's out there now is just like the tiniest sliver, but when the Internet of Everything becomes quite normalized, and it's down to the clothing we're wearing, the appliances we're using in our homes, you know, obviously just our, you know, increasingly powerful mobile capabilities, whether it's the watches we wear, or the phones that are in our pockets, etc. There's gonna be almost limitless array of data. And I don't think the private sector, for example, has done the job of essentially establishing what the norms and rules are, you know, most of the big media companies that are focused on this space or data companies have a kind of move fast, break things philosophy still, even though we're well past that point, I think in the maturity of those industries and the power that they have. There is some extended ability to arbitrage that which is to say if the Special Operations Committee can acknowledge the importance of this especially in a great power context, and say we want to be leading and defining the new laws of arms online and autonomous conflict are the new kind of LOAC the new Just War ethic.

Nick Lopez 50:40
That's about all we have time for today P. W. Singer in August Cole, thanks for coming on the Irregular Warfare Podcast, talking to us about "Burn-In" and sharing your thoughts for the future.

August Cole 50:50
Thanks for having us on.

P. W. Singer 50:51
Yeah, thanks so much. Really appreciate it. And great to connect with you. Take care.

August Cole 50:56
Thanks for doing the podcast. This is gonna be awesome. It's a great, great, obviously subject and thread to keep going or keep listening.

Nick Lopez 51:00
Thanks for listening to Episode Eight of the Irregular Warfare Podcast.

Shawna Sinnot 51:07
We release a new episode every two weeks. In our next episode, we will discuss the importance of organizational culture in units that conduct military advising with Dr. Austin Long. After that, we will talk the human domain of warfare with Brigadier General retired Kim Field and Dr. Sue Bryant.

Nick Lopez 51:24
Please be sure to subscribe to the Irregular Warfare Podcast so you don't miss an episode. You can also follow and engage with us on Twitter, Facebook, or LinkedIn.

Shawna Sinnot 51:33
One last note what you hear in this episode are the views of the participants and do not represent those of West Point, the Army, or any other agency of the US government.

Nick Lopez 51:41
Thanks again and we'll see you next time.