Cyber War Crimes
Professor Tarah Wheeler

30 March 2021

I am beyond overwhelmed at the kind introduction. Thank you so much, Simon. And it's an honor to be here with you all today to speak on the topic of cyber war crimes. Thank you, especially to the US/UK Fulbright commission, and to all of you listening today, let's get started. The kind and incredibly generous introduction aside. It takes some kind of strange people to end up having conversations about cyber warfare for a living. And let's not say for fun. I have spent my time learning to do a range of both risky and interesting behaviors like poker or flying planes, learning how to ride a motorcycle in the middle of a pandemic to be fair. I think all of us picked up a couple of strange hobbies over the last year or so, and yet the nature of what keeps happening in the headlines keeps pulling us back again and again in front of our computers. We see on an everyday basis that there is the rumblings of something beginning to happen, something dangerous and different.

I think the UK has stepped out really in front of the curve when it comes to the nature of cyber warfare in explicitly declaring the nature and beginnings of the National Cyber Force. I've had a conversation with some of the people involved in this process and in this project, and the United Kingdom is fortunate to have some of the most dedicated, brilliant, kind--let me repeat--brilliant cyber professionals that are known in the world. And it's an honor to get the chance to meet with them during this process. And as we see these headlines and we see the increasing nature of the threats that are building and bubbling on the internet and starting to merge into what we isn't, we can't even really call it real life anymore. This is real life. This is where we're sitting. You're sitting right now watching me in front of a computer probably right now.

That makes this experience as real for me and for you as it is for anyone trying to have a communication or have a conversation with anyone on the internet and as real as anyone beginning to enter a power grid or a water supply station or hospital, the way we think about these headlines, the way we think about the kinds of cyberattacks that we know are beginning, have been carried out, and are ongoing. Now, they don't have a framework. They don't have a way that we think about them in terms of other events for severity. We can't place them in the world on a lot of levels because it's still so hard to think of so much of this as real, right? The reason I'm in the United Kingdom right now, and here at the incredibly kind invitation of the US/UK Fulbright commission is to explore what happened during WannaCry in 2017 here at the National Health Service. The NHS dealt with what is without any hesitation, the most devastating potential and actual harm to human beings that has been conducted so far in a cyberattack. The fact that it's a nation-state cyberattack makes it an act of war. We're going to go through more of what that means over the course of this conversation. But I think I can begin now. And in this conversation, we'll start to answer the questions about not just "what is an act of cyber war," but when is someone actually going to die from all this?

I know I remember the first time I started to think to myself that the act of sitting down at my computer every day had started to become an act of violence, an act of prevention and active defense or offense. When that realization starts to hit home, we start to go from someone who's a cybersecurity professional, from someone who's in IT, to someone who thinks about the larger system, not just the computer sitting in front of me. I'm looking at a lot of screens right now, and they have started to mean something different to me over the course of the last several years, as I look more and more into the nature of conflict, especially over the internet. This is a world where people are trying to wreck my day

and yours every day in a new and interesting and horrifying way, but there are ways to make it better.

There are ways to keep yourself safe; there are ways to understand what's happening. So to start this conversation, this framework of how we begin to think about cyber warfare, let's start by looking at the nature of war itself, how it's developed over time and where this even fits in the concept of what would constitute warfare.

We started a long time ago, hitting each other over the head with rocks. And as war started to really develop, the concept of the dimensionality of warfare evolved right alongside it, whether you're talking about the battle of Salamis or any of the heroic engagements of the past on land. We're often talking about a unidimensional situation where you can see your opponent, attack them, and exchange visible blows. And there's a single dimension of warfare.

If we want to add that second dimension of warfare and ask ourselves what would be, what would it be like? Not just to fight along a straight line, but to fight on a plane, we might move from the battle of Salamis to something a little bit more like the battle of Actium or Trafalgar. We might move to the water. All of a sudden we can conceive of the notion of expanding the dimensionality of warfare from a straight line to a plane where the amount of real time-distance between you and your opponent started to decrease as the ability and speed of the vessels and transportation increased. So this is a once upon a time story, right? Once upon a time we were limited to land war. Then we were able to fight on water. Well, now, if your opponent gets that Navy, they can make war upon you from a further distance, as well as in another dimension. And what happens when all of a sudden we add a third dimension into the concept of warfare, we begin to add the battle of Britain we add in the third dimension, and all of a sudden, not just the space of warfare increases, but the friction points to reaching your opponent decrease again. All of a sudden having a mountain range in the way of you and your enemy doesn't necessarily stop you from going to war.

So adding this third dimension into the concept of warfare gets us right up until about 1945, 46. And then we started to ask our ourselves what if we added an additional dimension of space? And that concept of spatial warfare took us from Salamis to Trafalgar, to, uh, the battle of Britain. And all of a sudden, here we are in missile defense and star Wars and the space race. In this additional dimension, we've added the rotation of the earth's orbit into the way that we go to war. That's that additional dimension for space. And with that, the other belligerent in the conflict with you might become too indirectly positioned around the globe to really engage with as meaningfully anymore. Yet we now find ourselves adding an additional dimension of warfare where not only is your opponent potentially too far away or too unreachable, like in space—they might become unknowable.

The concept of cyberwarfare is one in which you're not necessarily always 100% sure who you're fighting. That dimension has always been there a little bit in warfare from simply the concept of asking yourself whether or not, you know your enemy. Knowing your enemy and not fearing the results of a hundred battles thereafter, as Sun Tzu said, is a part of, of military philosophy for millennia. And there's always been that question of whether we know our opponents, but I think we've always mostly thought about it in terms of the mind, as opposed to whether or not we can actually correctly identify them guerrilla warfare and the evolution of bringing more and more people into additional conflicts has started to elide the concept. This perfect vision of a uniformed enemy combatant on the field of battle that you can clearly identify as following a set of rules who is going to abide by the Geneva conventions…doesn't exist anymore.

We now find ourselves in this world where the other belligerent has become a form of unknowable

that we struggle to encapsulate because all of the ways that we've conceived of warfare. It involves first knowing who your enemy is before beginning to predict their actions or their motivations as well as that concept of becoming more familiar, more comfortable with predicting the actions and likely motives of an enemy without ever having identified them. This is a real challenge in our new conceptions, in new doctrines of warfare. This is how we're ending up at a place where we're not sure who we're going to war with, but we might actually be getting more competent at going to war to begin with. So after we have this conversation about the increasing dimensionality of warfare, after we think about how it is that that we can conceive of an opponent, then we need to ask ourselves not just who an enemy is in cyber warfare, but whether or not we're actually at war with someone.

So what is legally cyber war? In the United States, there is a bright line, a clear definition of what constitutes an act of war. There are small windowless rooms where people conduct these kinds of operations in the United States. It's very common to have a small group of people who are writing scripts, executing them and engaging in Title 50 espionage—flatly, countries around the world engage in espionage. There are two codes of law in the United States, Title 50, and Title 10 that govern espionage and warfare in the United States. Legally, for as long as you are merely listening and not engaging in destruction and deception on foreign shores, you are engaged under title 50, the laws of espionage and what are legally allowed to be done when listening in on an opponent. The second that someone hits an enter key, the second that the electromagnetic signal is sent from someone striking an enter key that executes a script that changes something on a server in a foreign country that either destroys information or changes the way people would behave or engages in shutting down a plant or any of the ways that you can conduct cyber warfare by attacking especially industrial control systems—in that moment you have stepped in that moment from Title 50 to Title 10 in the United States, and that has now become legally an act of cyber war.

These moments, the moment when you hit that enter key have become so important that at this point I am given to understand by people who would know that they require the same kind of sign-off from the Judge Advocate General Corps in the United States, and the same kind of sign-offs on a forward action that an act of kinetic warfare would. Hitting a single key in the United States that moves you from Title 50 to Title 10 is an act of war, and it is treated with that gravity. I fear on occasion that many of the kinds of people that engage in cyber warfare in rogue nation states around the world, revel in a lack of definition, because cyber war is often very difficult to define. That clarity of definition in the United States may mean that that there's a challenge in trying to determine when the appropriate moment has come to move from espionage to actual kinetic forward action.

So cyber warfare might be a little harder to define colloquially, but I can tell you this cyber war crimes are not hard to define. They're the same as every other war crime, because they intentionally direct attacks against civilian objectives, specifically objectives that are not military objectives. We're going to talk in a moment about a couple of acts of war that are legally, as far as anyone's been able to tell me, actual cyber war crimes. Cyber war crimes are not difficult to define under the Rome statute of the international criminal court. Article seven, which governs crimes against humanity and Article eight, which governs war crimes define very clearly what constitutes a crime against humanity. A war crime and conducting inhumane acts of character intentionally causing great suffering or injury to body or mental or physical health is a crime against humanity.

A war crime specifically targets civilian populations or against individual civilians not taking direct part in hostilities, especially places like historic monuments, hospitals and places where the sick and wounded are collected provided that they are not military objectives. This matters. And it matters because the United Kingdom has been the victim of a cyber war crime. WannaCry in 2017 was unhesitatingly a work crime committed by North Korean military hackers. And just because it was a sloppily conducted war crime (we'll talk more about how sloppy it was) doesn't mean that it wasn't

intentionally directed against civilian objectives and spilled over into harming hospitals. So we know that war crimes exist and we already have the framework in place that specifically defines why it is that something that is done by a nation state. A kinetic attack directed against a hospital is a war crime.

And yet it's so difficult to get that agreement. Why is it difficult to get that agreement? Why is it difficult to do anything under NATO's Article 5? It's difficult because Article 5 requires unanimity and flatly, unanimity is a difficult thing to come by in our current—we're not going to say quite post-Westphalian—order. As a result, we find ourselves in a world where we might just begin to ask ourselves, can we just take all this stuff offline? Can't we stop making ourselves targets? Can't we move from a world where we don't understand what's happening to one where we do?

Let's talk about that next. One of the questions I often get is “if I can't see this happening, and I can't see anyone around me affected by it, and I have no idea it's occurring and no one I know is being killed by it…Is this real? Is it actually affecting me in any genuine way?” I think what we have started to realize over the last year now is that the actions of other people impact us far, far more than we really have processed as a world and as a global community. The question of whether or not cyber warfare impacts individual people used to be a complex one, but it used to be one where you had to answer it with statistics and probabilities. For the first time, especially over the last three and a half to four years, we can point to specific individual examples of human beings who have been physically personally harmed by acts of cyber warfare. I'm going to talk a little bit about what exactly constitutes the weapon. What is a cyber weapon, how is it employed, how is it engaged and who is impacted by it?

This is the reason, again, that I'm here in the United Kingdom. It has to do with the fact that WannaCry happened in 2017. The interviews that I'm conducting here, the conversations I'm having with people are telling me now that there is a deep and hidden wound from the beginnings of this form of warfare. That has not yet been counted. It's not been something that we've processed as a globe. As people in the United States, as people in the UK, we haven't processed what it is yet. We haven't processed the fear and frustration that started in the middle of May, 2017, when WannaCry, the ransomware attack that originated from North Korea hit servers around the world. Any unpatched computer that was running Windows 7 was potentially vulnerable to this particular form of really awful ransomware. It shut down the machines, it shut down hospital equipment, it harmed accounting firms & legal firms, and stopped logistics from operating: WannaCry was a devastating attack. And if you don't really know yet how it impacted you, then we're still talking about statistics, but I can tell you that the NHS knows and remembers, and the IT personnel that I've spoken to at the NHS who remember that day, they remember it like someone in the United States would remember where they were when Kennedy got shot, or when they first heard on September 11th and the World Trade Center, coming down. People in it who did incident response that week remember where they were when they got the call in that same kind of way. It's starting to spill over into the kind of trauma that you see people processing after dealing with years of conflict zones. But what actually is the concept of a cyber weapon?

How does it work? What are these things? What are am I talking about when I say a ransomware attack? What do I mean by that? A ransomware attack tries to get onto your computer and find a bunch of files and encrypt them, and then ask you to pay to have your files decrypted. Interestingly, you never actually have your files taken from you. Usually in previous forms of this particular kind of attack, you usually didn't have your files stolen from you. Instead, you were denied the use of them. So what would happen is a worm would get onto your computer. We call it a worm when it's able to travel through computer systems and jump from system to system, as opposed to a virus which can

be carried by a worm, but a worm is more a form of transport.

So when this kind of attack happens, you are denied the use of your files on your computer, and that could be trivial. It could be that you just bought it. There's nothing on it yet. Or you could be someone who has a lifetime's worth of photos that you just digitized. And the most heartbreaking things that, that many of us heard that weren't related to human harm, or at least physical human harm, where people who lost the photos of their loved ones who had passed away, people who lost their small business records and couldn't pay their taxes that year. There's no doubt that was WannaCry which was the big boss of the kinds of ransomware attacks that blossomed after the National Security Agency of the United States lost a trove of cyber weapons. There's no doubt that the human impact was real and devastating. Once you see that happen, it's not something that really goes away from you.

And so it started to impact people in the real world. And so that's the beginnings of what these weapons do, but what does one actually look like? How do you hurt someone with a computer? So the first thing that you have to do is recognize that all of these things have to do with how computers work. They ask a question, and if it's answered one way, they do one thing. And if it's answered another way, they do another thing. Computers are simple. They're simple, but they'll follow instructions perfectly. So when I talk about the two main cyber attacks that we kind of use now, as examples of ways that people have gotten hurt, we talk about WannaCry and shortly thereafter, NotPetya. NotPetya was a Russian attack that was designed to attack Ukrainian accounting software in order to damage the logistics and penetrate the networks of the Ukrainian government.

And you can read accounts of what this worm did by far smarter people than me. Both of these things were styled, both WannaCry and NotPetya were styled as ransomware attacks. The truth is that NotPetya looked that way, but was a vicious and perfectly precise cyber weapon that then spilled over into shutting down 40% of the world's shipping in the matter of just a few weeks. Maersk, the global shipping conglomerate, lost billions of dollars and Mondelez International, the food and logistics provider, lost and tried to claim on insurance hundreds of millions of dollars in damages from food rotting in shipping containers around the world. There's no doubt that these kinds of attacks are impacting people. They're spilling into what we think of now as real life. But again, how do you do this with code? What are these things?

So here are the two cyber weapons I'm going to show you today. This is the real deal. That's NotPetya that shut down Maersk International. It took over Ukrainian servers spreading around the world in the blink of an eye. It was a precise, clear, and demonstrable use of force. So when you look at this code right here, I want you to see how logical it is. It is a simple loop that goes and looks for a process, tries to figure out if that process is running. And if it is, it asks some questions has the file. That's attached to what I'm looking at right now, and has already been encrypted. If it has skipped to the next one, if it hasn't tried to encrypt it, see if that'll work, then it tries to encrypt it.

You see up there a little do, if-do, and it jumps down. What that's saying in that loop is if this thing hasn't been done yet, try to do the thing. And if you can't do the thing, step to the next thing, as long as it's true that we're in this loop (that's the while down there) and as long as this condition is true. Keep trying to do the thing. As soon as it stops being true, and you've encrypted everything you can here, jump to the next moment, jump to the next place. You can start doing this again. That is as, as we would say, an elegant weapon from a more civilized age, it's, it's beautiful. It's precise. It's nation state level.

Now, this is what hit the NHS in 2017. That is WannaCry. It's a wreck. As a professional, I'm offended

by looking at it. This is what frankly probably got let out of a cage, possibly unintentionally, because it's so bad. It might've been an accident. And yet there's, there's a saying that goes around, which is that most experts agree that the most likely way the world will be destroyed is by accident, right? So when you look at this code, I want you to see that it looks like a wreck. This doesn't look precise. This is Stormtroopers falling all over themselves with no precision in anything they're doing. Do you see that function down there at the bottom? It says, uh, local underscore six c. And it leads to a specific function. That code, that comment right there, that sub-routine does not return. That was in the original code and the original code that was being analyzed in the days of May 12th, 13th, 14th, 2017.

It turns out it was being analyzed in Devonshire by a young man named Marcus Hutchins, who went by the name “MalwareTech”. Well, that was his finest hour. He registered the domain that made that sub-routine return and stop infecting other computers. It means that what he did was found something that we call a killswitch. It's common for people to embed domain names in bad code. When I say bad code, it’s not just bad code, but malware as well, one tries to control it. It makes it so that if you need to, you can reach out as the original author of that code, flip a switch and stop it from operating anymore. It stops the ticking timer that you see in movies on a bomb that's counting down. And you find out where the clip or the wire that presumably only the person who built it knows where it's located.

Well, it was hanging out there with a tag that said, cut me to stop this. And Marcus found it and hit that killswitch. And there's your finest hour. A young British man saved the world that day. And he stopped hospitals in the United Kingdom from shutting down. It was an extraordinary act and so far, it's probably the clearest act of cyber heroism we're going to see any time soon. And it's a pleasure to know him. This right here is mustard gas. It was indiscriminately released on a civilian population. The consequences are still there. And we're going to talk more about how WannaCry has a long tail. It's still out there. Remember, the killswitch is still operational.

It's still stopping computers around the world from, from continuing to encrypt files that could use the original ransomware that was created that is called WannaCry. So we start to ask ourselves the question, if this is what's happening. If, if the world is complicated, if you could do this with code, if you could shut down shipping and harm hospitals, what on earth can we do about it? I'm going to start to answer that question in just a second. It doesn't matter who you are. There is always something that you can do about this to protect yourself, to learn more, no matter what your skill set is or where you find yourself. I don't care if you're a school teacher or a lawyer, the most brilliant hacker in the world, whether you're a politician or somebody who just likes sailing boats around the world, it doesn't matter who you are.

There is still something that you can do about not only understanding, but beginning to start to prevent these kinds of actions of violence against a civilian population. So one of the things that we know about security is that no matter what it is never ever going to be perfect, we are never going to find a world where it's, there's no security gaps. It's just never going to be perfect, no matter what. And yet, one of the things we also know is that, although I've just told you that story about WannaCry and how devastating it was locking up NHS hospitals, and performing the kinds of cyber attacks that stop global transportation, food supplies for making it to where they need to be, prescription medication from making it to the right locations. We also know that though the patch has been released for WannaCry for the underlying flaw that made WannaCry possible.

We also know that of the companies that were vulnerable to WannaCry in 2017, 26% of them still are. That means more than a quarter of the companies that knew about found out about WannaCry and still have those same exact machines still haven't updated them. Why might they not have done that? Why might they not have updated those machines? For many people, they don't understand that the

nature of updating a computer is something that needs to be constant in the background, automatic, and always turned on for others. They deliberately chose not to update their computers specifically because they may be running things like critical infrastructure, which by itself is a terrifying conversation to have. If you are so dependent on a particular computer running for years at a time and can't restart it or can't change the software that's on it may be because it's running something as critical as water or power supply or an educational district.

And the reason you can't restart it, a computer running Windows 7 is because you're so reliant on it for provision of services that you can't afford, the time to repair it is why we end up with these kinds of cyber attacks. I definitely encourage anybody who has the eye, the ear of the folks in it to take a look at whether or not you're still running Windows 7. You can fix an extraordinary amount of the world simply by patching for this one vulnerability. We also know no matter what, that everybody has constant, ongoing incidents and vulnerabilities. There is no company, there's no organization, no government, no person who is 100% security flaw free. I, I'm not a great hacker. I'm a fine mediocre hacker. And I'm pretty good at making sure my own computers and situation is as secure as it can be. And yet I get hacked too.

I don't just have my data stolen in the same kinds of attacks that you do, Equifax or the kinds of breaches happen to governments. For instance, the OPM hack in 2014 in the United States or other data breaches that can become devastating, loss of email or address books like the Yahoo hack in the early two thousands. I'm pretty good at securing my stuff. And I get hacked. There's no shame in it, right? There's no shame in the fact that people who are smart and targeting one person in particular, or even just statistically trying to grab the maximum number of victims, they can find the way to harm you. We haven't stopped those impulses in humanity yet. That is why no matter what, there will always be ongoing security problems, flaws, and a reason to keep upgrading and patching. But that doesn't mean that we stop trying.

It doesn't mean that we stop trying to make the world better. It just means we acknowledge our limitations and then start working within them to improve the situation we find ourselves in, and that 25 or 26% statistic right there, we could do better, folks. We could do a lot better on that one. These are still people running critical infrastructure that need to patch and improve and upgrade. So when we ask ourselves the question, what can we do about it? Especially if we are IT professionals, if we're people who speak to IT pros, I can tell you this right now, the single best defense against ransomware is impeccable planned and scheduled backups (offsite backups), because it turns out that when people have an incident, a ransomware incident, most of the time, the reason that that data is so valuable is because there's no backup for it.

Anyone who has a full, complete, nightly backup of all of their data who experiences a ransomware attack, gets to thumb their nose at whoever engaged in this attack against them. Of course, people who have constant, ongoing, nightly backups and updates also usually have their patches rolling as well too. But this is a thing that you could do as an IT pro or as people who want to learn more about what IT pros do. You don't want data backup. You want restore, you want that ability to hit a button and restore your systems to a point in time. Plan for it, or ask the people who can do it to plan for it. Think about the way that your organizations, your governments, your companies retain and secure their data. We have to think about the fact that data retention becomes a liability over time, as well as a product of a lot of companies.

This is the stuff that international attackers go after. These are the keys to the kingdom: customer data, financial information. That's what people are going after. And the way that we think about data and the value that it holds for us is also being thought about by the people who want to take it from us. Consider the idea that data restore might be an option for you as an IT professional, or as

someone who thinks about whether or not your organization is appropriately set up in the event of a disaster. I'm always happy to talk more with you about this, but this is the kind of thing that a smart professional is thinking about right now. And this is the defense in depth that makes attacks by nation states, against companies, nonprofits, hospitals, governments, and individuals, communities so difficult, especially if you've thought about this in advance.

What can you do about it as a, as a policymaker, as someone who thinks about these problems on everyday basis to try to keep other people safe. I have a great friend and mentor who once said to me as I was busy, rebuilding my computer for the sixth time that month, trying to get a driver to work. I was fascinated by this one thing and irritated by it. And he said, you're running a company. Now, you don't have time to do everyone else's job. Do your job and let other people do theirs. So this is the question I have for you as someone who needs to talk to people about how to do their job: think about how you store your data. Think about what you're doing to protect yourself individually against these kinds of ransomware attacks, NHS hospitals, US hospitals, shipping conglomerates, banking, legal legal firms, governments everywhere have to start having these conversations about data, retention, data architecture, and data security. And remember that sometimes the best choice in security to purge or delete, or be able to audit and keep that data might be in direct conflict with things that we treasure like privacy or the right to move freely without surveillance. These are tough choices and no one's pretending they're not.

Don't give up on it. We went straight from, from hese giant concepts, these global attacks, the big concepts of the battle of Salamis and the idea of missile defense and global cyberwarfare to what you personally do in terms of data, structure and choices. But that's because this is a war coming to a laptop near you. This isn't something that you can avoid as a subject or a topic any longer, and talking about how international conflict impacts you and your family and your government and your organization and your company is something that we're all going to have to start doing. Think about how you'll balance choices between being able to verify something or audit something versus protecting individual privacy. And the rights of the user is—well, that's frankly the question we've all been asking ourselves in Silicon Valley, in the United States, and the global information security community for decades.

Now, none of these are easy choices. Maybe use a little bit of a thought experiment. The next time you go to the doctor, ask your doctor “what happens to my data? If I tell you I want it, or I want you to delete it?” Then, figure out—just ask yourself and then ask them, “do you even know what’s happening to my data?”

Just remember that the things people are stealing, the things nation states are removing from you or taking from you, or denying your right to access is personal data, as well as international or strategic data. No matter what, all data is going to eventually become either deprecated or deleted away, or it will become fully public. And in the hands of a foreign power, nothing stays secret forever. Data either totally loses its value, or it becomes a part of the historic record. So which one do you want?

The data that you're protecting? These are the questions that are being asked by people at the Pentagon or GCHQ. Everyone is starting to ask themselves because these kinds of conflicts are local now, or so global as to be indistinguishable from something that you see everyday on the street. So what don't you know, about the way the world is going to start working, not just today, but tomorrow? So we've talked about what constitutes this kind of warfare. We've talked about what makes up these cyber weapons, how they're being deployed, how they're being used. And just some of the questions you can ask yourself about how you keep yourself safe. There's no one perfect solution that applies to everyone, but you can use some of the questions I just gave you to ask, not only yourself, but the people around you, how to keep yourself safe and how to make smart choices to reduce your own

attack surface.

In the event of the kinds of attacks that we're seeing increasingly dedicated towards people, companies, organizations, there's no border anymore for cyber warfare to be directed at—nothing that stops someone from targeting you directly. And so these are some of the ways that you can ask these important questions, no matter who you are, some of the ways you can frame these questions. So we know what's happening today, but what's about to happen tomorrow. Well, we have now gotten to a point where we have seen the very first AI powered cyber attack. This was done in India at a bank with the usage of natural language processing and a phishing attack that was automated by use of a data breach. And the information that was found within it was massively successful. And we're already seeing the automation of these kinds of attacks in actual practice.

So what's going to happen when they start becoming more and more common? We're going to see an increasing flood of traffic that is illegitimate and yet difficult to both define and stop because these kinds of attacks look like every other email that you'll see. Paying attention to how information security professionals think about phishing attacks and personal safety will help. But the truth is we're now at a policy level. Again, we've now gotten back to the point where we're not asking questions anymore about what switches we flip as people, but how we think about either as policymakers or as people who want to speak to policymakers about what the world is going to look like.

These are not acceptable numbers. These are not acceptable numbers because they start to tell us that the companies that are protecting our data aren't doing the kind of job that they should be. These are solutions that happen at a policy level with regulatory frameworks, that penalize companies for letting loose our personal data on the world, because they can be used in cyber attacks against us. It's not appropriate for companies to face little to no penalty for the kinds of negligence that lets the world be damaged on a permanent and ongoing basis. We're beginning now to see the kinds of attacks that are bearing fruit after seven to eight years of data leaks in Malaysia Airlines, in the Starwood breach from several years ago, and the kinds of attacks that are beginning to go after a high net worth traveler's data.

These are beginning to float around the internet. Take a look and you'll see what I'm talking about. These solutions are at a policy level. They're at the international level. Again, think about and ask yourself whether or not it's appropriate for companies to face no penalty. Don't be that company. And if you're not that company, make sure that company faces a penalty for the kinds of negligence that hurts you and your family on an ongoing basis. We're already there. We're already at automated warfare. And yet it's a little frightening to think about how difficult it is sometimes to understand these concepts in cyber warfare, that they're happened, that they are impacting people, that there's no border. There's no fort stopping these kinds of attacks from rogue states from penetrating national borders and going straight after civilian targets. We know that these kinds of attacks are happening, and we know that they're going to continue to devastate us over time.

And yet we're not developing enough systems thinking, enough of the kinds of thinkers and kinds of people that can solve these problems. Partially because technology and information security still has a massive diversity problem. And when I say that, I don't just mean the color of someone's skin or their gender. I'm talking about the kinds of people who think about problems differently. We sometimes use diversity as a catchall term for trying to make sure that we're seeing what we need to see in reality. It's about thinking in new and interesting ways, the kinds of people who come up with these ideas, not only to do horrific things in authentic, but brilliant things in defense, they don't think the same as everyone else. Sponsor, mentor, educate, promote fund, and train that diversity. That difference in thinking. And that's how we're going to start to see a way to combat this kind of

automated warfare.

We're going to see a way to begin to combat the kinds of attacks that go after civilians. Find a way to think differently and be open to listening to people who are involved in the world and thinking about cyber warfare in different ways than you're thinking about it. We know this isn't going to end, right? This is not a situation that's going to stop. A hundred percent of companies have ongoing incidents. 0% of security is ever perfect or is ever going to be, and this isn't going to end. This isn't new in the way many people think about it. It's just the continuing story of conflict and fraud at the international level of harm against civilians and protection and militaries. These are stories that go back to Herodotus and Thucydides. They're not stories that are new in any way, other than the fact that we're using a computer to conduct warfare.

And so just remember that just as the story of humankind contains these stories of war and pain and fear, so also they do contain the stories of people who came up with ways to save the world, a killswitch, penicillin. The way that we save the world is by that same kind of new thinking, that also helps us come up with the defenses against the kinds of attacks that are harming civilians. This is why I'm sitting here today. I have enjoyed talking with you today. The truth is this is such a somber subject that I don't know if “enjoy” is even the right word. I'll tell you though: I feel privileged to sit here today and speak with you about it and share ideas. I look forward hopefully to being able to speak with you as well, one day, and I'm going to give you my contact information in just a moment. It’s a big topic, but you're probably watching this alone. Well, you're not alone. We're out here. We're thinking about ways to solve these problems. And I want to hear from you. I want to know how I can refine my thinking and how we can make this world a better place. I look forward to speaking with you. I am again, so profoundly honored and grateful that the US/UK Fulbright Commission asked me to be here. That Gresham College saw fit to introduce me so kindly and provide this platform. I'm gratified and humbled, and we'll all keep thinking as hard as we can about this problem. And you're not alone. I know I'm not alone. We are working together. We're trying to make it better. It will happen. We can do it. It was a genuine pleasure. Have a wonderful day. Thank you.

© Professor Wheeler, 2021

Further Reading

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations.* (2017, Oxford University Press).

Healy, Jason, ed. *A Fierce Domain: Conflict in Cyberspace 1986-2012.* (2013, CCSA)

Tarah Wheeler, “The danger in calling the SolarWinds breach an “act of war”. 4 March 2021. https://www.brookings.edu/techstream/the-danger-in-calling-the-solarwinds-breach-an-act-of-war/
T. Wheeler, “The vaccine supply chain is now the most valuable cyber target in the world” 18 March 2021. https://slate.com/technology/2021/03/world-health-organization-vaccine-cybersecurity-censure.html
T. Wheeler, “In Cyberwar there are no rules: why the world desperately needs digital Geneva Conventions” https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/
T. Wheeler, “NATO, we want to go to war with you”. https://foreignpolicy.com/2020/12/22/nato-we-want-to-go-to-war-with-you/