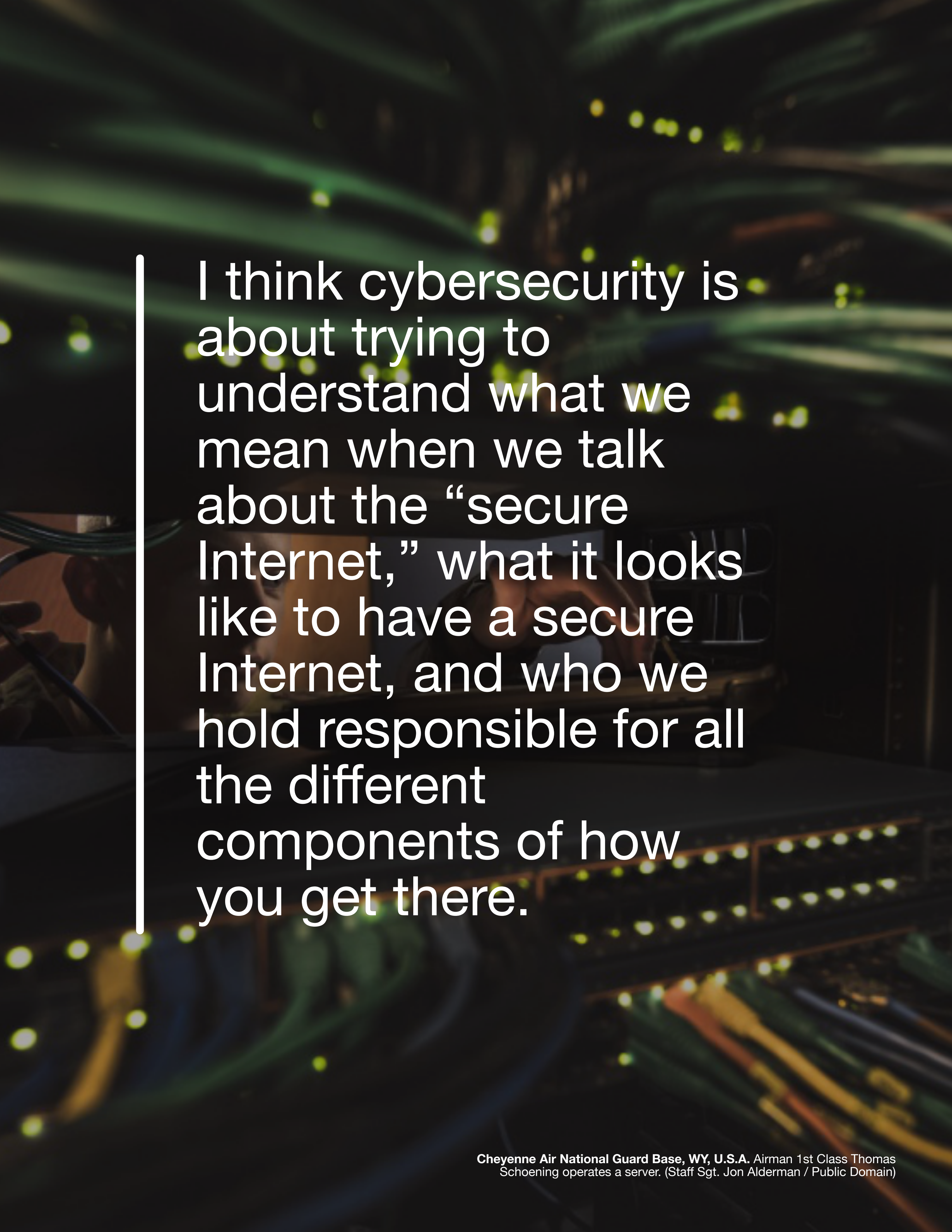


I think cybersecurity is about trying to understand what we mean when we talk about the "secure Internet," what it looks like to have a secure Internet, and who we hold responsible for all the different components of how you get there.

Cheyenne Air National Guard Base, WY, U.S.A. Airman 1st Class Thomas Schoening operates a server. (Staff Sgt. Jon Alderman / Public Domain)

Cybersecurity: State Attack and Response Strategies

A Conversation with Dr. Josephine Wolff

Interviewed by Ta-Chun Su

Fletcher Security Review (FSR): Professor Wolff, thank you very much for speaking with us today. To begin, can you start by explaining what cybersecurity as a discipline means for you?

Josephine Wolff (JW): I think my focus has always been on looking at the intersection of technical, social, legal, and policy levers around cybersecurity. One of the questions that has always been very interesting to me is "Who do we hold responsible when something goes wrong with cybersecurity?" While that is a technical question—because often when something goes wrong, there is a technical component since you are dealing with a computer and the Internet—it also very much has to do with what our liability regimes say, what our policies say, what our social norms and expectations say about who we hold accountable and who is expected to pay for the damage. So for me, I think cybersecurity is about trying to understand what we mean when we talk about the "secure Internet," what it looks like to have a secure Internet, and who we hold responsible for all the different components of how you get there. To whom do we say "It's your job not to answer the phishing emails," or "It's your job to look for bug traffic on the network." How do we piece together that entirely complicated ecosystem of different stakeholders, and how do we identify what their different roles and responsibilities should be?

FSR: Are liability regimes different for different kinds of incidents?

JW: Absolutely. Think about the different kinds of things that can go wrong in cybersecurity. For example, right now we have a lot of ransomware attacks, where somebody will encrypt a hard drive or even get an entire organization or city's hard drive, and the victim will be unable to access any of their data held captive for an extortion demand, usually for digital currency payment. The questions here should be about who should be responsible, who should pay for that, how do we cover those costs, and how do we deal with it. But it is totally different than what happens if there is a big data breach, like with Equifax, where 147 million people's data got stolen. Who we hold accountable and how we deal with it is totally different if we are looking at something like a denial-of-service attack, when you are bombarding a server with so many packets that it goes down. That is technically a very different thing, but it is also very different in terms of the policy space.

FSR: In the case of Equifax, we run into some tricky issues: we do not know how the stolen data will be used, the cost of the harm is hard to measure, and we are incapable of putting those perpetrators, in this case military officers from the Chinese People's Liberation Army (PLA), into jail.

JW: The question is what is the appropriate response? We cannot really do anything after the fact to try to hold the responsible party accountable.

FSR: In this case, is it considered economic espionage?

JW: Yes. That is what the Justice Department has called it.

FSR: China has been engaging in espionage efforts to steal data and intellectual property. From both the corporate and government perspective, how could we better combat such efforts?

JW: When we talk about espionage broadly, a lot of technical emphasis is placed on network segmentation—so that it is harder to get access to part of the network—and monitoring data exfiltration, which is the moment when data is leaving the network. Then there are broader questions about what you can do after an incident of espionage, because there are all sorts of midpoint-interruptions. One proposal that was introduced several years ago in the U.S. Congress was the Deter Cyber Theft Act, where the idea was that the U.S. government should keep a list of companies in China or anywhere else that have stolen U.S. intellectual property and, as a result, should be banned from doing business in the United States. We should try to have economic consequences, because the ultimate goal of economic espionage is economic benefit. But, of course, there are a lot of implementation obstacles to overcome in order to actually make that happen.

FSR: Then, if the harm is already done, is it easier for us to target attackers during the later stages of the process?

JW: That is the big thing I work on. It really depends on what kinds of attack you are dealing with. That is the argument I made around a lot of financially-motivated cybercrimes. It is easier to focus on that monetization stage. And if you are trying to interrupt, there are only a few ways to make money out of stolen data– either you are going to sell it or you are going to use it.

FSR: I think you have written about this regarding credit card fraud, right?

JW: Exactly. I think the espionage is more complicated. Look at the Equifax breach, we think the government of China has information on 147 million people, but no one really knows

Suffolk, VA, U.S.A. CAPT Julia Slattery, commanding officer of Navy Cyber Defense Operations Command (NCDOC), answers questions about the Equifax breach. (Rebecca Siders / Public Domain)

what they want to do with it. They probably want to steal money, because that is usually what the Chinese government does. With Westinghouse, we have a slightly clearer sense that they were stealing the piping plan for their nuclear power plant, because they probably want to make a nuclear power plant themselves or sell that kind of intellectual property. But it is harder to determine what is going on in the case of Equifax.

FSR: In your book, you sort cybersecurity breaches into three categories according to the motives of attackers—financial gains, espionage, and revenge. What are the reasons for these classifications?

JW: I did that because I am interested in these later stages of intervention, which are often where policy and legal efforts are focused. Figuring out how to interrupt monetization is really only a relevant question if the criminal was trying to make money. My theory is that these later stages of attacks are based predominantly on the overarching motivation for the perpetrator, so that's why I divide them by motivation. Is your motivation that you want to steal money? Is your motivation that you want to conduct espionage? Is your motivation that you want to publicly shame or exact revenge on your target in some more nebulous way? One of the things I found useful about doing this was it allows us to stop looking at these incidents purely through the technical lens and saying, "These are all phishing attacks, because phishing can be used for all of these." The tech techniques are absolutely interesting—all of those technical access points—and I think those are all important things to think about. How do we do a better job of dealing with phishing? How do we deal with all these technical vulnerabilities? But I think that organizing incidents that way is less useful if you are interested in the policy piece, because policy is probably not how we are going to stop phishing, right? That is not the thing that law enforcement or governments are going to turn out to be really good at. What they are going to be good at is thinking about how we deal with money moving around, or how we deal with stolen secrets being used, and these really require looking at the end goals of the attackers.

FSR: Is there any clear-cut or distinct line between economic espionage and political espionage?

JW: It is a really good question. I have a lot of trouble with it. I think there are some cases where it is really clear cut. There are two examples I usually use because they happened around the same time and they are both attributed to the Chinese government. The first is the 2015 Office of Personnel Management breach, in which information, like security clearance information for millions of current and former U.S. federal employees, was stolen along with their fingerprints. This is very useful political espionage information—you would know everything about everyone who is working for the U.S. government. While it is attributed to China, there is no indictment. There is none of this legal song and dance because it is political espionage; the United States tries to draw this line between economic and political espionage. Right around that moment, about a year earlier, they filed this indictment with Westinghouse, U.S. Steel, and all those other allegations. Their contention was that this is not like the good kind of espionage that we all do. This crossed a line because it is a government stealing intellectual property on behalf of its own domestic businesses. So, if the example is stealing nuclear power plans, that is economic espionage, but stealing information about the United States and U.S. government employees and spies, that is political espionage. Then you look at something like Equifax though, and there are charges of economic espionage in that indictment, but it is not obvious to me that personal information about 147 million people is an economic advantage as opposed to a political one. So I think you do start to see some blurring, especially when you have a country like China, where the distinction between state and commerce is not as clear.

FSR: For example, companies like Huawei, which is mostly controlled by the Chinese government, right?

JW: Exactly, so I think it is neither obvious to them nor people who look at their system. Of course, there is this clear dividing line between "this is what we do for the government and this is what we do for our industry." The United States has pushed really hard for the norm that economic espionage is not okay in the international system while political espionage is, but I would say they have not been very successful. I think it is often complicated depending on the structure of a country and the structure of its private sector. I do not think there is any kind of international consensus on whether one form is okay as the cyberspace norm while the other is not.

FSR: Given the dense linkages between the United States and China, how can the U.S. government prevent or mitigate the Chinese espionage effort?

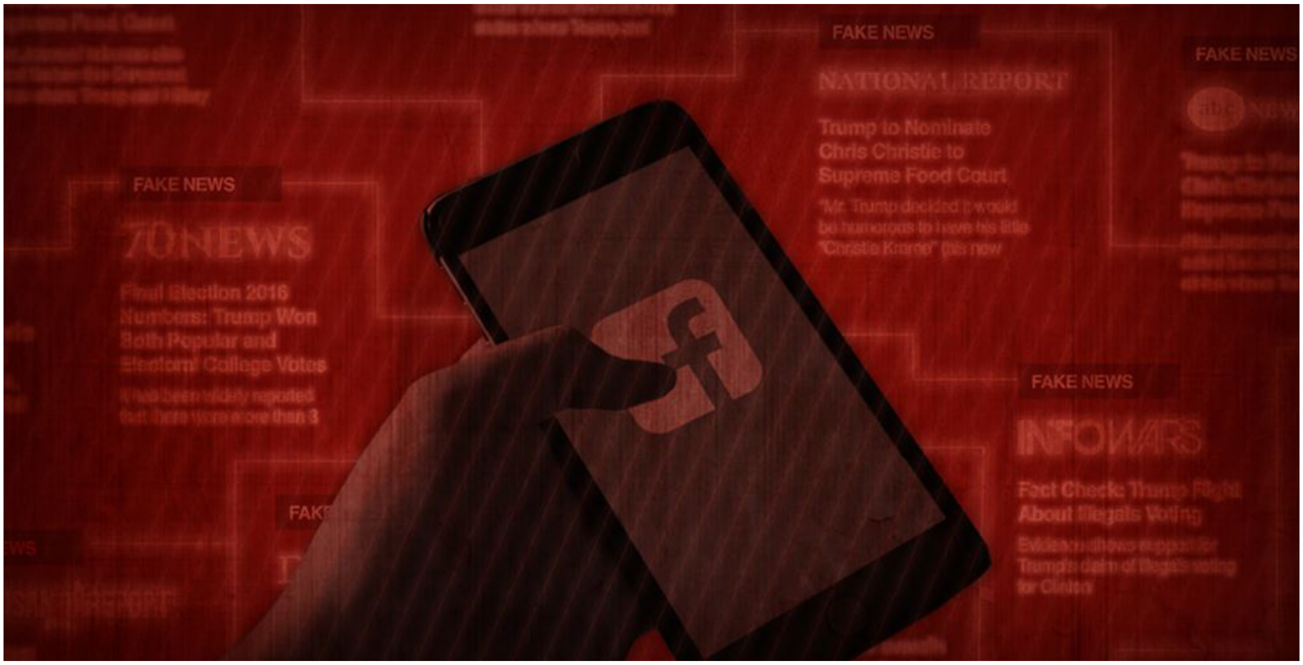
JW: It is a great question. I wish I had a better answer to it. I think there are economic consequences that could be meaningful. I think it is part of the trade war that we have just seen between the United States and China, but it is only one part of a much messier situation between the two countries. It is hard to say how much of that is about economic espionage versus everything else that is going on. I do think economic consequences for economic espionage makes sense. I think that is one way of trying to impose penalties, especially when you are dealing with China, which cares very much about its economic growth. The problem is that for it to be effective, the United States has to impose consequences in a very clear and consistent way, which is not how they have done it to this point, right? Everything that we have just seen in the past year or so between the United States and China has been so messy, raising questions like, "Why is the United States doing this? What do they want?" For penalties to work, I think the economic consequences have to be, "Okay, this company took this piece of intellectual property, and therefore they are not allowed to sell their products or their services in the United States." We have not seen very clear economic sanctions of that kind. What we have seen are a couple of these indictments in the name-and-shame strategy. I think there is value to doing that not because it seems to deter China from conducting espionage, but because I think there is value in publicizing what their tactics are and how they do what they do for defensive purposes. I think right now, especially when the United States is very focused on trying to convince other countries not to use Huawei and all these other things, there is some value in the signaling that these indictments provide: "Look at what China is doing. Be aware of that." So I think there is some value in those responses, but I do not know how effective they will be. The last time we did this in 2014, the United States filed an indictment against several People's Liberation Army officers for espionage. Then there was a summit between President Obama and President Xi and there actually was some improvement in the espionage relationship between the two countries. And then we had a new administration, and that progress deteriorated very quickly. So it is very cyclical; it is not clear that these are long-lasting agreements.

FSR: I suppose there is no blueprint behind the U.S. strategy.

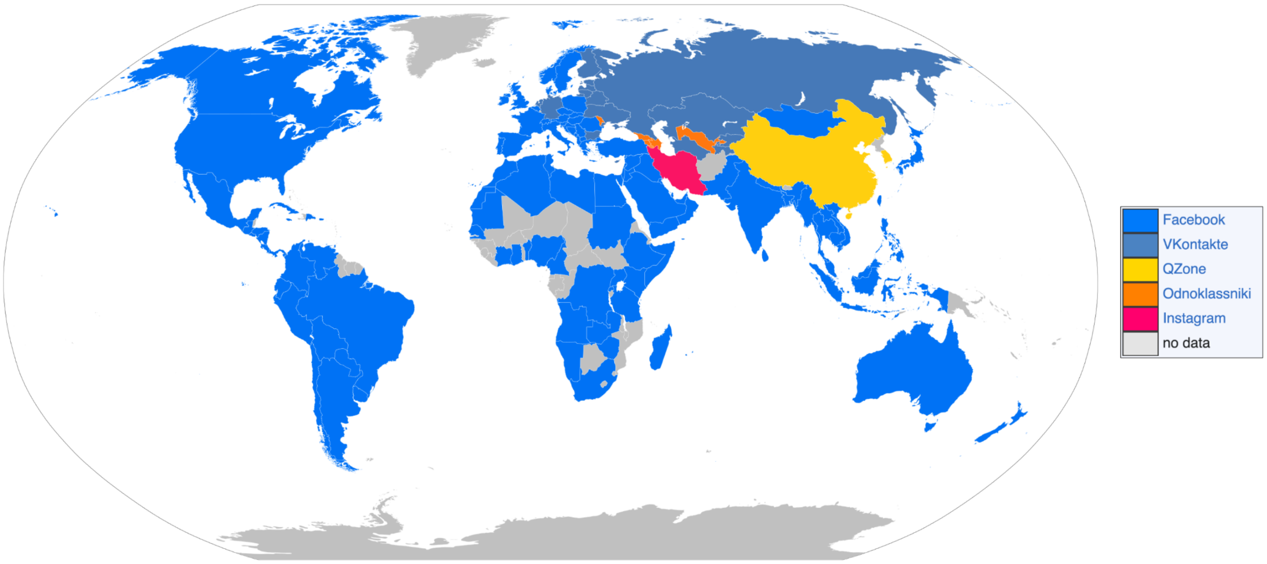
JW: Yes, we do not have a very good guide for how to do this, I would agree.

FSR: Let's move on to the propaganda and misinformation campaigns. We know that Russia and China have actively engaged in recent efforts to interfere with democratic elections. How and through which channels does this work? For example, China used cyber operations to help a pro-Beijing candidate win a local election in Taiwan in 2018.

JW: I think it is always changing. It always depends on what platforms people are using. In the 2016 election, there were a lot of people on Facebook and Twitter, so that was where the


FAKE NEWS
NATIONAL REPORT
Trump to Nominate Chris Christie to Supreme Food Court
FAKE NEWS
70NEWS
Final Election 2016 Numbers: Trump Won Both Popular and Electoral College Votes
FAKE NEWS
FAKE NEWS
INFOWARS
Fact Check: Trump Right About Illegals Voting

"It always depends on what platforms people are using. In the 2016 election, there were a lot of people on Facebook and Twitter..." - Dr. Josphine Wolff (Graphic by VOA News / Public Domain)



Most popular social networking site by country 2019. Data sourced from Alexa's Top 500 Sites. (Christoph Friedrich / CC BY-SA 4.0)

Russian misinformation campaigns were. I think as those platforms change, you will probably see the misinformation tactics change as well. I will say I know less about China's misinformation involvement. My sense is that it is more internally focused, that it is more about providing misinformation to people within China, than it is about persuading people outside of China. I know there was a Facebook release about posts that the Chinese government likes.

FSR: There are many fake accounts that have been spreading fake news around Taiwan.

JW: So I guess internally—I mean mainland China, Taiwan, Hong Kong—that there has been a fair bit of interest in that area, but I don't know of examples that are akin to the Russian involvement in the U.S. election in which China's trying to influence the outcome. I think that is a really interesting case of a combination of cybercrime and social media manipulation. There is real criminal activity that happened, like stealing information from the Democratic National Committee, and then it is coupled with this campaign that is largely protected under free speech protections in this country. So you get this complicated collision between what is free speech on these platforms and what is the obligation of these companies to regulate whether the things that are said on them are actually true, which is a pretty big obligation for platforms the size of Twitter or Facebook. That is a lot of material that they are going to be expected to vet, and then there is the added complicating layer of the ads from which they make money. I think there are a lot of questions about who is responsible for what, and all of them come back to this question: "What do we expect our platforms to take care of in terms of misinformation?"

I have a lot of sympathy for people who feel that those companies could do more and I also have some sympathy for the companies, which feel like, "There are millions of people using our platforms, are we really supposed to figure out every stupid lie that one of them is posting?" I think it is certainly fair to say they could do more than they have. I also get why Facebook is not eager to get into the business of deciding which political ads are true and which ones are false, because as soon as they start doing that they start alienating certain groups of people, which they are clearly very concerned about because they want their user base to be as large as possible.

FSR: It is a tricky problem to address.

JW: These are not companies run by people who wanted or intended to be making political or policy decisions. These are people who wanted to build technology.

FSR: It is difficult to strike a balance between personalization and privacy. Tech companies have long tried to personalize their services and offer tailored content for users, but personalization comes at the cost of privacy.

JW: Yes, I think the personalization question is very complicated because it depends on what you are personalizing. Most of what we see in this space is personalized ads and it is not clear there is really any benefit to the consumer from that personalization. Unless they are showing you something that you really want to buy, I suppose.

FSR: But what about Netflix and Spotify, for example, using recommendation algorithms to build loyalty followings?

JW: Yes, and there is maybe more benefit to you to have some of those recommendations that might actually help you find something you did not know about that you really enjoyed. So I do not think all personalization is bad by any means. I think one of the trends we are seeing, especially in the European Union, is toward a little bit more control over how your data is used and what kind of data is being used for that personalization. I think on the whole, that is a good thing. For example, the General Data Protection Regulation (GDPR) is intended to give you a little bit more autonomy and a little bit more transparency.

FSR: But the core principle of GDPR, which is user consent, cannot be considered meaningful if they do not enjoy genuine choice.

JW: I think that is one of the drawbacks. And one of the drawbacks is that when you are trying to get somewhere on the internet, you do not want to stop and read a long message that somebody is flashing at you on the screen, you just click "OK" and you move on. I think all of those are real obstacles: Do you really have the choice to opt in? Did you really pay any attention to the information? And if you did pay attention, was there really anything very specific or detailed in there that told you anything more than, "We use your information to improve our services" and whatever else? I think the principle is a good one and the direction is a positive one, but I think we still have a lot of implementation details to work out.

FSR: And the enforcement is also patchy because there are 28 countries, right?

JW: Absolutely. There are even more data protection agencies than that, because some countries have multiple data protection agencies and each of them has its own agenda and its own decision-making authorities, and they do not really coordinate. In the sense that the European Union passed the GDPR, it is a regulation at the level of all of them, but each country has to implement it individually. And we see very different behavior out of the different countries. Ireland so far has not issued a single fine under the GDPR, but many countries, such as the UK and France, have.

FSR: Does France have more stringent requirements?

JW: We don't know yet, because we do not know what Ireland is ultimately going to do. I think there are also differences, like the fact that the French Data Protection Agency, I believe, gets to keep the money that it fines to fund the agency, whereas the German data protection agencies do not. So that is a very different incentive for how much you are going to fine and all of the structures are a little bit different from country to country. It is, I think understandably, a little bit hard for companies to keep up with all of them and figure out how to navigate everything, even though it is all one regulation at the EU level.

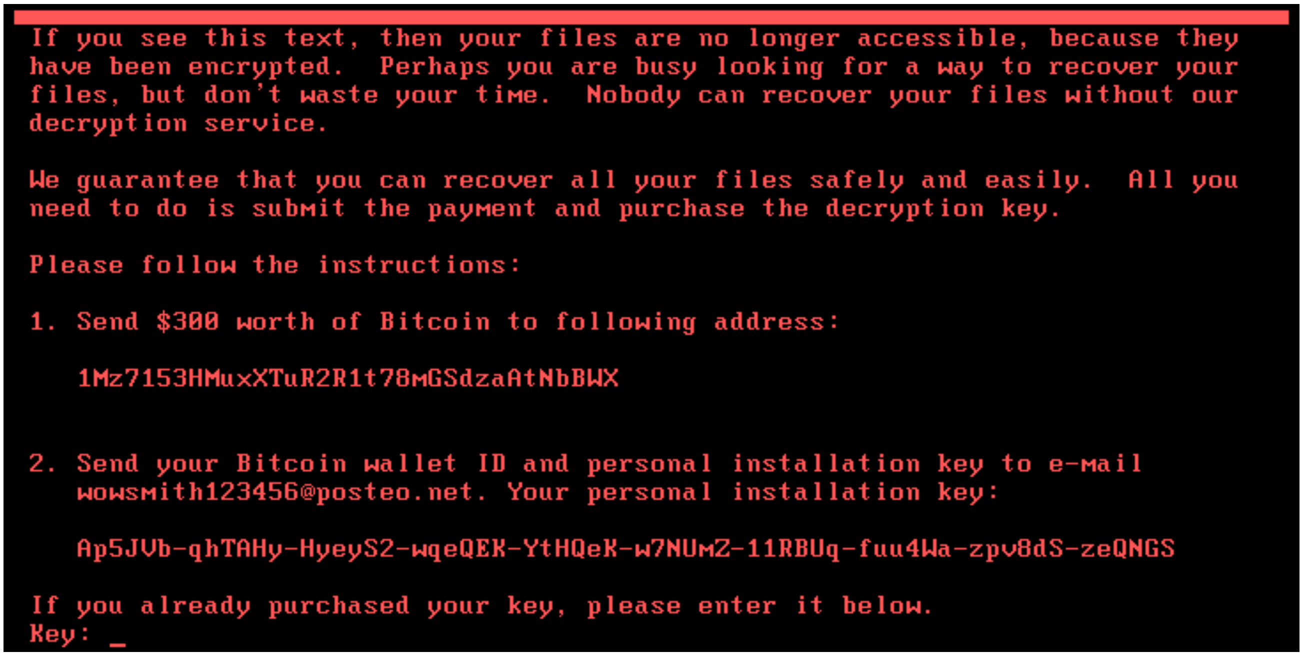
FSR: But some big tech companies are not afraid of being fined, compared with the benefits of flouting those laws and rules.

JW: I think that is fair. I think a lot of the fines are small enough that the big tech firms would not care too much. GDPR does enable fines of up to 4% of annual revenue, which is quite a lot of money for a large tech company. But yet, we have not seen a Google or Facebook fined 4% of their revenue. That would be an unheard of fine in this space. But one of the points of GDPR was to leave that option on the table. And so far, the largest fine we have seen is to Google for 50 million euros, which is much less than 4% of its revenue.

FSR: Now the EU Commission is exploring what a post-GDPR world might look like. Its emphasis seems to shift from stopping bad companies from doing bad things to actively encouraging good companies to do things.

JW: I think there is a mix from data protection agency to data protection agency. I do think it is true that a lot of the GDPR enforcement we have seen has not been looking at what happens when things go wrong when there is a data breach, but rather how clear is your privacy policy? How much are you obeying the spirit of the GDPR and the transparency in use restrictions, which is definitely a shift from the previous regulatory regime and also a shift from the regulation that hap-

"...we see very different behavior out of the different countries. Ireland so far has not issued a single fine under the GDPR, but many countries, such as the UK and France, have." - Dr. Josephine Wolff (Graphic by Dooffy Design / Public Domain)



```
If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   Ap5JVb-qhTAHy-HyeyS2-wqeQEK-YtHQeK-w7NUmZ-11RBUq-fuu4Wa-zpv8dS-zeQNGS

If you already purchased your key, please enter it below.
Key: _
```

Screenshot of the Petya ransomware demand. (Unknown / Public Domain)

pens in the United States around data privacy and security.

FSR: In terms of liability, can you talk more about the respective roles of state and non-state actors in preventing cybersecurity breaches?

JW: I think when it when it comes to thinking about liability, the role of the state is to try and make things clear, to try and say, “the internet service providers are responsible for doing this, the retailers collecting people's data and payment information are responsible for doing this, and the individual users are responsible for doing this.” And there has not been a lot of that clarity. We have seen some progress, but most of it has come at us in a sort of piecemeal, case-by-case way. I think this is because when you are dealing with the Internet, you have such a complicated ecosystem, right? There are so many different kinds of companies involved. When you send packets over the Internet, you have an Internet service provider, usually multiple service providers, who are carrying those packets. If you are buying something, you have a platform like Amazon or Facebook that you are using to make the purchase through. So there are all these different companies involved and it is understandable that unless there is some sort of clear policy and legal precedent around who is responsible for what, all of them are going to kind of feel like this could be somebody else's job.

FSR: We do not have many precedents to look for, right?

JW: There are more than there used to be. A lot of what I do is look at some of those incidents and say, “Okay, when there is a big data breach of payment card numbers, what does the retailer pay for? What does the credit card company pay for? What do banks pay for? How do we split that up over all the different actors involved?” But it is a complicated setup, and I think the messiness of it, the fact that all of these companies are so interconnected online, makes it harder than if you are, for instance, thinking about your car. If there is a car manufacturer and the cars turn out to be defective, who is responsible for that? That is a simpler question than if there is a denial-of-service attack or a data breach that touched 15 different stakeholders. Then who is to blame?

FSR: I think they just want to pass the buck. They just do not want to take the responsibility.

JW: Yes, but it requires thinking about liability in a more complicated way. It requires thinking about liability in a way that says, “Look, there is not one responsible party, there are a bunch of responsible parties who all had certain obligations in certain ways.” And that is really hard to do. That requires more complicated liability policy, and that is not something that is easy for them or is easy for the courts to do in the absence of their policy, I would say.

FSR: We often see policies and laws that have struggled to keep up with technical advances. Given the fact that cyberspace is dominated by mostly private actors, it seems that it is better to let private firms take the lead and regulate themselves.

JW: They always like self-regulation. I would say that self-regulation is really hard in the liability space because if you ask a company, “How would you self-regulate for liability?” Mostly they will say, “Well, we would self-regulate, but put the liability on somebody else.”

FSR: Are there any voluntary initiatives or codes of conduct?

JW: We have had some codes of conduct, for instance around bots, and there was something called the anti-bot code of conduct for Internet service providers, such as the Interactive Simulation Package. They do not work very well, on the whole. It is one thing to say here is a voluntary code of conduct for security, it is another to actually get anybody on board with following it. We have seen a lot of this breakdown. So I think there is truth to the idea that the private sector is really important in this space and that they have a lot of valuable input to give. But I am more wary of self-regulation, especially when it comes to security and liability, because I think that is the way that you get to the situation where everybody is pointing to somebody else and saying, “This was not our fault. This was the service provider. This was the content provider, this was the DNS operators,” and there is always somebody else to point to.

I think part of what has been complicated about liability in the space is that companies are very wary of assuming any voluntary responsibility because then they will be the only one who does. Governments will start to look to them and say, “This is your fault. You said you were going to be responsible for this." There is a first-mover problem—nobody wants to be the first type of company to step up and say, “We are going to take responsibility for battling bots.” Again, I have a lot of sympathy for that, but I think the solution, or part of the solution, has to be this carving up of the responsibility and saying, “Okay, you are responsible for looking at malicious traffic, because that is something you can do really well. You are responsible for looking at fraudulent payment transactions because you are a payment processor, and you have a lot of insight into that. You are responsible for looking at vulnerabilities in software because you are a software manufacturer.”

FSR: Is there any regime that has been built before?

JW: Well, the way it is usually done is that as things happen, you start to sort it out incident by incident and a certain amount of that is always going to be the case, because every incident is a little different. But I think we could provide clearer guidance than we do currently.

FSR: Can you talk a little bit more about global Internet cooperation and governance, and some of the challenges there?

JW: I would say the biggest overall challenge is that different countries have very different ideas about what a secure Internet will look like. Until you have some consensus around that, you cannot really work toward it as a common goal. For instance, an example would be around cybercrime. The United States and many other countries would say a secure Internet is one where it is very difficult to commit cybercrimes and when you do, it is possible to catch you and put you on trial. That has not really been the stance of say Russia, which is a place where many very powerful, very wealthy cybercrime syndicates operate. Because it is a global network, if you do not have every country or almost every country on board with that as a norm, then all the cyber criminals are operating out of Russia and the United States can issue as many indictments or charges as it wants, but nothing is going to happen because there is no cooperation there. So I think the global Internet governance challenges have largely boiled down to the fact that there is just not actually consensus on what we want the Internet to look like and what we think the priorities are for security. As long as there are a few holdout countries saying “We are going to do things our way and not your way,” it is really hard. If everybody has different ideas about this, we do not have a lot of time to figure out whose ideas are better.

FSR: Speaking of the United States, it seems that they have no robust regulatory regimes in terms of preventing cybersecurity breaches.

JW: The United States does not have comprehensive cybersecurity regulation in any way. They have bits and pieces that relate to certain types of data. For instance, there is a law around children's data and how that needs to be protected and collected, there is a law around health data, and some laws around financial data, but there is nothing that is the equivalent to the GDPR that says, “Here is our regime for data protection across the board.”

FSR: But there is an act called the Computer Fraud and Abuse Act (CFAA).

JW: But that is not a data protection law. That is about illegal hacking. The Computer Fraud and Abuse Act says, “If you access computers without authorization or an excessive authorization, that is illegal,” which is a complicated thing because it raises a lot of questions about when you are authorized to access computers. There is a whole body of case law out there in which people try to figure out what is illegal hacking, but that law is meant to go after criminals, which only works as long as you can actually get those criminals—when you can actually arrest them and bring them to trial. Sometimes you can, but not always in the Internet ocean. There are plenty of people tried under the CFAA, but there are plenty of people that are not.

Dr. Josephine Wolff

Dr. Josephine Wolff is an assistant professor of cybersecurity policy at The Fletcher School. Prior to joining Fletcher in 2019, she was an assistant professor of public policy at the Rochester Institute of Technology, a fellow at Harvard’s Berkman Klein Center for Internet & Society, and a fellow in New America's Cybersecurity Initiative. Dr. Wolff’s research interests include international Internet governance, cyber-insurance, and security responsibilities and liability of online intermediaries. She received her Ph.D. in Engineering Systems and M.S. in Technology & Policy from MIT, and an A.B. in mathematics from Princeton University. Her book *You’ll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches* was published in 2018 by MIT Press.