
# Interview: Kim Zetter

Cybersecurity journalist **Kim Zetter** talks with *Limn* about infrastructure hacking, the DNC hacks, the work of reporting on hackers and much more.

**Christopher Kelty: So our first question is: What kind of technical or political thresholds have we crossed, and have you seen, in your time reporting on hacking and information security? Is Stuxnet [2010] a case of such a threshold, or the DNC [Democratic National Committee] hack? Since you've been doing this for a long time, maybe you have a particular sense of what's changed, and when, over the last, say, decade or so?**

Kim Zetter: I think we have a number of thresholds in the last decade. And the DNC hack definitely is a threshold of a sort. But it's not an unexpected threshold. There's been a build up to that kind of activity for a while. I think what's surprising about that is really how long it took for something like that to occur. Stuxnet is a different kind of threshold, obviously, in the military realm. It's a threshold not only in terms of having a proof-of-concept of code that can cause physical destruction—which is something we hadn't seen before—but also it marks a threshold in international relations because it opens the way for other countries to view this as a viable option for responding to disputes instead of going the old routes: through the UN or attacking the other nation, or sanctions or something like that. This is a very attractive alternative because it allows you to do something immediately and have an immediate effect, and also to do it with a plausible deniability because of the anonymity and attribution issues.

**CK: Why do you say this is long overdue?**

**KZ:** With regard to the DNC hack, we've seen espionage and political espionage is not something new. The only thing that's new here is the leaking of the data that was stolen rather than, let's say, the covert usage of it. Obviously, the CIA has been involved in influencing elections for a long time, and other intelligence agencies have as well. But it's new to do it in this very public way, and through a hack, where it's almost very transparent. You know, when the CIA is influencing an election, it's a covert operation—you don't see their hand behind it—or at least that's what a covert operation is supposed to be. You don't know who did it. And in this way, [the DNC hack] was just so bold.

But we've seen sort of a step and progression of this in the hacking world. We saw when Anonymous hacked HBGary [2011] and leaked email spools there. We saw the Sony hack [2014] where they leaked email spools. And both of these put private businesses on notice that this was a new danger to executives. And then we saw the Panama Papers leak [2016], where it became a threat to wealthy individuals and governments trying to launder or hide money. And now that practice has moved into a different realm. So that's why I'm saying that this is long overdue in the political realm, and we're going to see a lot more of it now. And the DNC hack

is a bit like Stuxnet in that it opens the floodgates—it puts a stamp of approval on this kind of activity for nations.

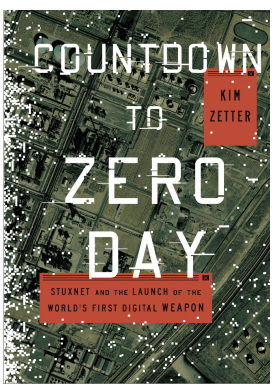
**CK: This is at the heart what I think a lot of people in the issue are trying to address. It seems that the nexus between hacking as a technical and practical activity and the political status of the leaks, the attacks, etc., is somehow inverting, so there's a really interesting moment where hacking moved from being something fun...[with] occasionally political consequences to something political...[with] fun as a side effect.**

**KZ:** Right. I've been covering security and hacking since 1999. And we started off with the initial hacks; things like the "I Love You" virus, things...that were sort of experimental, that weren't necessarily intentional in nature. People just...testing the boundaries of this realm: the cyber realm. And then e-commerce took off after 2000 and it became the interest of criminals because there was a monetary gain to it. And then we had the progression to state-sponsored espionage—instead of doing espionage in the old ways with a lot of resources, covert operatives, physical access, things like that. This opened a whole new realm; now we have remote destructive capabilities.

**CK: So, let me ask a related question: in a case like the DNC hack, do we know that this wasn't a case of someone who had hacked the emails and then found someone, found the right person to give them to, or who was contracted to do the hacking?**

**KZ:** Yes. I think that's a question that we may not get an answer to, but I think that...you're referring to something that we call "hybrid attacks." There are two scenarios here. One is that some opportunistic hacker is just trying to get into any random system, finds a system that's valuable, and then decides to go find a buyer, someone who's interested in [what was obtained]. And then the stuff gets leaked in that manner. If that were the case in DNC, though, there probably would have been some kind of exchange for money, because a hacker—a mercenary hacker like that—is not going to do that for free.

But then you have this other scenario, where you have what I'm referring to now as hybrid attacks. We saw something similar in the hack of the Ukraine power grid [2015–2016], where forensic investigators saw very distinct differences between the initial stages of the hack, and the later stages of the hack which were more sophisticated. The initial hack, which was done through a phishing attack in the same way [as the DNC was hacked], got them into a system and they did some reconnaissance and they discovered what they had. And then it looks like they handed the access off to more sophisticated actors who actually understood the industrial control systems that were controlling the electrical grid.




Kim Zetter is the author of the definitive book on the StuxNet virus, *Countdown to Zero Day* Broadway Books, 2015.

And they created sophisticated code that was designed to overwrite the firmware on the grid and shut it off and prevent them from turning it back on.

So there is a hybrid organization where front groups are doing the initial legwork; they aren't necessarily fully employed by a government or military, but are certainly rewarded for it when they get access to a good system. And then the big guys come in and take over.

When you look at the hack of the DNC and the literature around it—the reporting around it—they describe two different groups in that network. They describe an initial group that got in around late summer, early fall, around 2015. One group gets in and then the second group comes in around March 2016. And that's the group that ultimately leaked the emails. It's unclear if that was a cooperative relationship or completely separate. But I think we're going to have this problem more and more, where you have either a hybrid of groups cooperating, or problems with multiple groups independently being in a system. And this is because there are only so many targets that are really high-value targets, who could be of interest to a lot of different kinds of groups.

**CK: What I find interesting about hacking are some of the parallels to how we've dealt with preparedness over the last couple of decades, independent of the information security realm. You know, thinking about very unlikely events and needing to be prepared, whether that's climate change–related weather events or emerging diseases. Some of the work that we've done in Limn prior to this has been focused on the way those very rare events have been restructuring our capacity to respond and prepare for things. Is there something similar happening now with hacking, and with events—basically starting with Stuxnet—where federal agencies but also law enforcement are reorienting around the rare events? Do you see that happening?**

**KZ:** I suppose that's what government is best at, right? Those big events that supposedly we can't tackle ourselves. So I think it's appropriate if the government focuses on the infrastructure issues. And I don't mean just the critical infrastructure issues like the power grid and chemical plants, but the infrastructure issues around the internet. I don't think that we should give it over entirely to them. But in some cases, they are the only ones that actually can have an influence. One example is the FDA [U.S. Food and Drug Administration], and its recent rules around securing medical devices for manufacturers and vendors who create medical devices. It's so remarkable to think that there was never a security requirement for our medical devices, right? It's only in the last year that they thought it appropriate to actually even look at security. But it shouldn't be a surprise because we had the same thing with electronic voting machines.

**CK: Yeah, it's a shock and laughter moment, it seems to repeat itself. Switching gears a little bit: one of the questions we have for you has to do with your experience in journalism, doing this kind of work. Do you see interesting new challenges that are emerging, issues of finding sources, verifying claims, getting in touch with people? What are some of the major challenges you've encountered as a journalist trying to do this work over the last couple of decades?**

**KZ:** I think that one of the problems that's always existed [in] reporting [about] hackers is that unlike most other sources they're oftentimes anonymous. And so you are left as a journalist to take the word of a hacker, what they say about themselves. You obviously put things in context in the story, and you say, "According to the hacker," or "He is a 20-year-old student," or "He's based in Brazil." There's not a lot of ways you can verify who you're talking to. And you also have the same kind of difficulties in verifying their information. Someone tells you they hacked a corporation and you ask, "Can you give me screenshots to show that you have access inside this network?" Well, they can doctor screenshots. What else can they give you to verify? Can they give you passwords that they used, can they tell you more about the network and how they got in? Can they give you a sample of the data that they stole? And then of course you have to go out and verify that. Well, the victim in many cases is often not going to verify that for you. They're going to deny that they were hacked; they're going to deny that they had security problems that allowed someone in. They may even deny that the data that came from them is their data. We saw that with parts of the DNC hack. And it was true that some of the data hadn't come from them. It had come from someone else.

**CK: Do you find that—do you think that—finding sources to tell you about this stuff is different for studying hacking than for other domains? Do you basically go back to the same sources over and over again once you develop a list of good people, or do you have to find new ones with every event?**

**KZ:** In terms of getting comments from researchers, those are the kinds of sources I would go back to repeatedly. When you're talking about a hacker, of course, you can only generally talk with them about the hacks that they claimed to have participated in. And then of course they can just disappear, like the Shadow Brokers. After that initial release and flurry of publicity, several journalists contacted the Shadow Brokers, got some interviews, and then the Shadow Brokers disappeared and stopped giving interviews. So that's always the problem here. Your source can get arrested and disappear that way, or willfully disappear in other ways. You may only end up having part of the information that you need.

**CK: We have a number of articles about the difficulty of interpreting hacks and leaks and the expectation that the content of the leaks will have an immediate and incontrovertible effect—Pentagon Papers-style, or even Snowden-style. A leak that will be channeled through the media and have an effect on the government. We seem to be seeing a change in that strategic use of leaks. Do you see that in your own experience here too? That the effectiveness of these leaks is changing now?**

**KZ:** You know, I think we're still working that out. We're trying to figure out the most effective way of doing this. You have the WikiLeaks model that gets thousands of documents from Chelsea Manning, and then just dumps them online and is angry that no one is willing to sift through them to figure out the significance of them. And then you have the model, like the Snowden leak, where they were given in bulk to journalists, and then journalists sifted through them to try and find documents and create stories around them. But in that case, many of the documents were still published. Then we have the alternative, which is the Panama Papers, where the data is given to journalists, but the documents don't get published. All we see are the stories around them. And so we're left to determine from the journalists: Did they interpret them correctly? Do they really say what they think they say?

We saw that problem with the Snowden documents. In the initial story that the Washington Post published about the Prism program, they said that, based on their interpretation of the documents, the NSA [National Security Agency] had a direct pipeline into the servers of these companies. And they misinterpreted that. But because they made the documents available it was easy for the public to see it themselves and say, "I think you need to go back and relook at this." With the Panama Papers we don't have that. So there are multiple models happening here, and it's unclear which is the most effective. Also, with the DNC, we got a giant dump of emails, and everyone was sifting through them simultaneously. The same with the Ashley Madison emails: everyone was trying to find something significant. There is sort of the fatigue factor: if you do multiple stories in a week, or even two weeks, people stop reading them because it feels like another story exactly like the last one.

And that's the problem with large leaks. On the one hand you expect that they're going to have big impact; on the other hand, the reading public can only absorb or care about so many at a time, especially when so many other things are going on.

**CK: The DNC hacks also seem to have a differential effect: there was the sort of Times and Post readers who may be fatigued hearing about it and who fell away quickly. But then there's the conspiracy theory–Breitbart world of trying to make something out of the risotto recipes and spirit cooking. And it almost feels like the hack was not a hack of the DNC, but a hack of the media and journalism system in a way.**

**KZ:** Yeah, it was definitely manipulation of the media, but only in the sense that they knew what media would be interested in, right? You're not going to dump the risotto recipes on the media (although the media would probably start up with that just a bit, just for the humor of it). But they definitely know what journalists like and want. And I don't think that journalists should apologize for being interested in publishing stories that could expose bad behavior on the part of politicians. That exists whether or not you have leaked emails. That's what leaking is about. And especially in a campaign. There's always manipulation of the media; government-authorized leaks are manipulation of the media as well.

**CK: I think I like that connection, because what's so puzzling to me is to call the DNC hacks "manipulating the presidential election" suggests that we haven't ever manipulated the presidential election through the media before, which would be absurd, [Laughter.] So there's a sort of irony to the fact that we now recognize it as something that involves statecraft in a different way.**

**KZ:** And also that it was from an outsider: I mean, usually it's the opposite party that's manipulating the media to affect the

outcome. I think they're all insulted that an outside party was much more effective at it than any of them were. [Laughter.]

**CK: Okay, one last question. What's happening to hacker talent these days? Who's being recruited? Do you have a sense in talking to people that the sort of professional landscape for hackers, information security professionals, etc., has been changing a lot? And if so, where are people going? And what are they becoming?**

**KZ:** The U.S. government has been recruiting hackers from hacker conferences since hacker conferences began. From the very first DEFCON, undercover FBI and military were attending the conferences not only to learn what the hackers were learning about, but also to find talent. The problem of course is that as the cybersecurity industry grew, it became harder and harder for the government and the military to hold onto the talent that they had. And that's not going to change. They're not going to be able to pay the salaries that the private industry can pay. So what you see, of course, is the NSA contracting with private companies to provide the skills that they would have gotten if they could have hired those same people.

So what's always going to be a problem is that the government is not always going to get the most talented [people]. They may get them for the first year, or couple of years. But beyond that, they're always going to lose to the commercial industry. Was that your question? I'm not sure if I answered it.

**CK: Well, it was, but I'm also interested in what kinds of international recruitment, what shake-up in the security agencies is happening around trying to find talent for this stuff? I know that the NSA going to DEFCON goes all the way back, but now even if you're a hacker and you're recruited by NSA, you may also be recruited by other either state agencies or private security firms who are engaged in something new.**

**KZ:** Right. In the wake of the Snowden leaks, there may be people who would have been...willing to work for the government before who aren't willing to work there now. And certainly Trump is not going to help the government and military recruit talents in the way that past administrations might have been able to appeal to patriotism and, you know, national duty. I think that that's going to become much more difficult for the government under this administration.

---

**KIM ZETTER** *is an award-winning, senior staff reporter at* Wired *covering cybercrime, privacy, and security. She is the author of* Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.

**Interview conducted February 2017.**