[SLICE OF MIT THEME MUSIC]

SPEAKER 1: You're listening to the Slice of MIT Podcast, a production of the MIT Alumni Association.

JOE MCGONEGAL: This is the *MIT Alumni Books Podcast.* I'm Joe McGonegal, director of Alumni Education. Fred Kaplan, who earned his PhD from MIT in 1983, is the author of *Dark Territory-- The Secret History of Cyber War.* The book chronicles America's search for IT order among cyber chaos in the last quarter century. Kaplan takes us through the effects of commissions and exposés, development of protocols and international scandals. His research unearths some entertaining anecdotes like this one.

In the late 1990s, when he started researching the vulnerability of infrastructure, Richard Clarke learned that 80% of global internet traffic passed through just two buildings in the United States-- one called Mae West in San Jose, California, and the other called Mae East, above a steakhouse in Tyson's Corner, Virginia. One night, Clarke took a Secret Service agent to dinner at the steakhouse, after which they took a look at the room upstairs. They were both shocked at how easily a saboteur could wreak devastating damage.

I reached Kaplan by phone and I asked him whether he chose to write the book now because we've finally purged ourselves of cyber scandals and reached a happy ending.

FRED KAPLAN: I chose the topic of this book before anybody had ever heard of Edward Snowden. My previous book, which came out in 2013, was called *The Insurgents-- David Petraeus and the Plot to Change the American Way of War.* And shortly after-- or maybe before, I don't remember-- it came out, my editor was talking to me about another book and asked, what's the new trend in warfare? And I said, well, there might be something to this cyber thing. And she asked what that was, and I loosely explained it. Quite honestly, I didn't really know-- yeah, I'd read a couple of books and a bunch of articles and things. I didn't know much about it myself. And before I decided to do that book, I did some research, talked with maybe 10 people, to see if there was a story there. And it turned out there was. And the contract was negotiated before the Edward Snowden revelations. That was a pretty big leap, in terms of public consciousness about the issue, so.

JOE MCGONEGAL: You delicately maneuver around issuing any judgments on the various entities of the US government who have engaged in cyber war. By the end of the book, you seem to feel at least

an inkling of patriotism for your country. Is that accurate?

FRED KAPLAN: You mean as opposed to Russia and China, Iran, and other countries? Yeah. But I would say that what I'm trying to do is-- and I did the same thing with previous books about other aspects of weird military things, like counterinsurgency and nuclear doctrine-- is to show the logic that created this way of thinking and why the people who think the way they do came up with their conclusions in a very logical way.

At the same time, I exposed some problems with this logic. I think in the case of things like the National Security Agency, the way that agency exists now-- one thing I discovered, and was surprised to discover it, is the place is crawling with lawyers who take the restrictions on what they do very seriously. You will not find anywhere, in the Snowden papers or very many other places, too, too many instances of actual abuse. You know, spying on political dissidents at home, that sort of thing.

At the same time, the potential for abuse is so massive given their intrusive powers. And it's not just theoretical. You know, in our recent history, going back to the '70s, there are plenty of instances in which corrupt presidents and ambitious CIA and NSA directors have interfered with our rights in shocking ways.

And so you know, if you could imagine, say, Richard Nixon and J. Edgar Hoover having this kind of technology available to them at the time-- or you know, let's get contemporary. If you can imagine a Donald Trump and Attorney-General Chris Christie having these kinds of powers, a lot of the restraints and the restrictions within the NSA were built up internally. Which means they can also be taken down internally with not that many people knowing about it. So the need for outside oversight is considerable.

JOE MCGONEGAL: What about this book becoming required reading in Iran or China military schools?

FRED KAPLAN: Well, there are 20 countries that have cyber units in their militaries. Are you asking if I worry that they might find out about things that their commanders don't already know? I don't think that's true.

JOE MCGONEGAL: These are things they already know.

FRED KAPLAN: Yeah, I would say this. There were a couple of things that I learned, or pieced together and

got confirmed, in the course of doing my research that I did not put in the book precisely for that reason.

JOE MCGONEGAL: Early on in the book, you talk about MIT's domain in the early world of hacking and national security concerns. It seemed like hackers loved routing through MIT.

FRED KAPLAN: Well, you know, at the time, when the internet was put up, the idea was, this is great for the free exchange of ideas and research among academic institutions. It started as the ARPANET-- in other words, especially academic institutions that, in one way or another, had military contracts. They were free and open. And therefore it is true that the early hackers would get into military networks by coming through portals, free and open portals, in academic institutions, and MIT was a favored, or mit.edu. And they would use that to go into, say, Lincoln Lab, and then from Lincoln Lab into the Department of Energy or Defense. Yeah, that is how the early hackers, going back to the mid '80s, really, how they started getting into national security networks.

JOE MCGONEGAL: Let's talk about some of the fellow alumni in the book. The most prominent, perhaps, is Richard Clarke, who was a contemporary of yours at MIT. Tell us a story you enjoyed learning about his work in Washington in the last 20 years. You've got the Five Guys commission. You've got-- even from a very early stage, he was a colorful character in the White House, no?

FRED KAPLAN: Well, you know, during the Clinton administration, he was the Counterterrorism chief. And you know, he's most famous for being the guy who stayed on that position into the early Bush administration. And he wrote the bestseller *Against All Enemies* and was the one who had been warning about the dangers of al-Qaeda and nobody listened. That's all well known.

But around this same time, he was put in charge of the cybersecurity account, as it became realized that our computers were pervasive and increasingly vulnerable to hacking. And he wasn't that interested in it, but he decided that, well, I've got this job. I'll look into it. And he was put in touch with a, quote, a "white hat hacker" who goes by the name Mudge. Peiter Zatko. He's very famous within this community.

And he went and met him in Cambridge and went to a place called The Loft that Zatko and four of his colleagues had built. And he saw in there that just using commercially bought equipment, they had been able to hack into passwords, replicate chips designed by other countries, hack into satellite communications. They claimed that they could shut down the

internet.

The point is, he realized that they were doing things, or at least had the capability of doing things, that the US intelligence community had said only nation-states could do. Clarke realized that this did fit into his portfolio, that if Zatko and his Loft crew had been pernicious, if they decided to be terrorists, they could be cyberterrorists. And that has shaped some of the scenarios that most frighten people today.

JOE MCGONEGAL: I was eager to look up Zatko in our directory, but of course you say he's a Berklee alum.

FRED KAPLAN: Yeah, he was an electric guitar major at the Berklee School of Music. He was sort of a self-educated computer genius. I think one thing that people are realizing is that hackers-- which used to be a nasty term-- are useful. Because these are the people who can identify threats very rapidly, more so than some, even smart people inside the crusty bureaucracy. So you know, right now the government and many companies pay bounty fees to private hackers who find vulnerabilities in their systems, because they'd rather pay somebody $100,000 to find a system rather than wait around for the Chinese to find it.

JOE MCGONEGAL: Bug bounties, we call them.

FRED KAPLAN: Yeah, yeah, exactly.

JOE MCGONEGAL: The customers who bought your book on Amazon also bought Richard Clarke's book, *Cyber War: The Next Threat to National Security and What To Do About It.* How is your book a revision of his?

FRED KAPLAN: Clarke wrote that book-- I think it came out in 2010. I remember the critical reaction to that book, which was even-- *Wired Magazine* wrote a review saying, file this under fiction. A lot of even the technology community thought it was just made up. I don't think anybody would say that today.

You know, Dick obviously was plugged in. He knew some things. I talked with more than a hundred people who are very, very deeply involved in this story, including six of the eight living NSA directors. There were also some documents that have come out since. Dick cut off a piece of that story and was the first person to do so. I don't think he would disagree that I've written a much more comprehensive history that goes back-- I mean, I identify the beginning

of this story going back to the beginning of the internet, back in 1967. And I bring it up to date, really right up to even a few weeks before the book came out a few months ago.

JOE MCGONEGAL: You also mention Larry Summers in there. There's mentions of Art Money and William Odom, who both studied at this the Sloan School. But talk about the contribution of Willis Ware, who earned a master's in 1942 from MIT.

FRED KAPLAN: Right. Well, Willis Ware, in 1967-- this goes back to the very beginning. The ARPANET was about to roll out. And he at the time was the head of the computer science department at the Rand Corporation. He'd worked with von Neumann on the first computers. He was also, though he didn't tell very many people this, on the Scientific Advisory Board of the NSA.

And he wrote a paper, and it was classified at the time. It's been declassified since, and it's a fascinating paper. He said, look, here's the thing. When you start putting information in a network, information where you give online access-- it might have been the first use of the word "online"-- online access from multiple unsecured locations, you're creating inherent vulnerabilities. You're not going to be able to keep secrets anymore.

In my research, I talked to the guy at ARPA who ran the ARPANET program at the time. And I said, did you read Willis Ware's paper? And he goes, oh, sure, I knew Willis. And I said, what'd you think?

And he goes, well, I took it to the team, and I talked with a couple of members of the team, too, to confirm this story. And they read it. And they said, oh, god, please don't saddle us with a security requirement. Look how hard it was to do what we did. It's like telling the Wright brothers that their first plane has to carry 20 passengers for 50 miles. Let's do this one step at a time. And besides, it'll take decades for the Russians to do something like this.

Well, you know, it did take decades, two and a half, three decades, by which time whole systems and networks had been created, had grown up, with no provision for security whatsoever. And I see this as sort of the bitten apple in the digital Garden of Eden. The kinds of things that we're reading about and experiencing today, a few people, like Willis Ware, saw as embedded in the system.

And years later, the two young men who wrote the screenplay for *War Games* came and talked with him to see if their scenario was plausible. In other words, could some kid just dialing into a lot of computer modems actually get into the main computer of NORAD?

And he said, well, you know I designed that computer, and you're right, it's a closed system. But there was always some officer who wanted to do work from home on the weekends, so they'd leave a portal open. And if a kid happened to dial into it, yeah, you could get connected. And then he leaned forward and he says to these guys, he goes, look, here's the thing. The only computer that's completely secure is a computer that no one can use.

JOE MCGONEGAL: Chapter 12, you describe the Stuxnet operation, which was handed off from George Bush to Barack Obama. And behind that, in part, was Richard Clarke's work, but also on the receiving end, I thought of Ali Salehi, a contemporary of yours also, from '77, got his PhD in nuclear science here. Vice president of nuclear policy in Iran. What do you think it was like for him on the receiving end of Stuxnet?

FRED KAPLAN: Well, I didn't know him. You know, I was in the political science department. But you know, it was a brilliant code, the Stuxnet. It was brilliant because not only did it alter the speed with which the centrifuges spun and therefore it destroyed them, but it also sent false messages to the people on the other end monitoring the system to make it look like everything was operating normally. And then all of a sudden, it just breaks. So you know, what the hell?

And you know, scientists were-- perfectly good scientists were fired for presumed incompetence. Perfectly good equipment was-- they looked for new sources of the goods. So they didn't know that anything was even happening until it spun out of control. They looked for-- the Israelis in particular looked for new ways to get in, and the bug spread around the world.

Now, it was designed in a way that if it interacted with any Siemens-controlled device, except for the one at the Natanz reactor, it wouldn't actually do any harm. But you know, people saw this bizarre bug and they looked into it, and as it was, a company like Symantec or Kaspersky, their whole job is to alert customers of bugs that are floating around. And they looked into this one and it soon became apparent what it was, and then the Iranians unplugged everything from anything that could be affected from the outside. But no, while it was going on, they just saw that they were having unexplained technical problems.

JOE MCGONEGAL: Talk about the status quo today. You don't have any mention in the book of the United Nations. Is that a place where cyber conversations should be happening, or should be happening more, if they already are happening?

FRED KAPLAN: Well, you know, theoretically, the UN could be a forum, but it isn't now. You know, this is where

the title of my book comes from. When Robert Gates became Secretary of Defense-- he was SecDef for the last two years of Bush and the first two years of Obama-- and he would get these daily briefings on hacks into Defense Department networks, defense industry networks.

He would tell some of his colleagues, he would say, look, we have to get together with the other cyber powers and create some kind of rules of the road, some targets that we can't go after with cyber weapons. You know, critical infrastructure, things like dams and things like that. He said, you know, even during the height of the Cold War, there were rules. The US and the Soviets, for example, agreed not to kill each other's spies. And they abided by this rule throughout the whole Cold War.

He said, you know, we're wandering in dark territory here. I remember looking at my notes and thinking, well, that's the obvious title of my book. But I looked it up. I googled the phrase, and I saw that it was a term of art in the North American railroad industry for stretches of track that were not guided by any signals. And I'm thinking, wow, that is a powerful metaphor for cyberspace.

And I sent Gates an email and asked him if he knew this. And he said, oh, yeah, my grandfather was a stationmaster on the Santa Fe Railroad for 50 years. We used railroad terminology all the time.

So it's true, we're in this state where, as I say, more and more countries, especially the United States, has everything hooked up to computer networks. There are crazy people out there, that this isn't anything that you need a Manhattan Project to do. You know, a room full of computers and people who know how to use them.

We have something called the US Cyber Command, which has war plans, which has targets, which is integrated with all other combatant commands. And we haven't thought at all about the most basic ideas. You know, as we speak, there is a panel of the Defense Science Board in the Pentagon writing a study on cyber deterrence.

When the atom bomb first went off in 1945, within a matter of a couple of months you had economists, social scientists, physicists, political scientists, thinking about, writing papers about, examining the question of how this new weapon in our midst changes, or doesn't change, the nature of warfare. With cyber, until very, very recently, everything about it has been so secret, way beyond top secret clearances. You had to have code words, specially compartmented clearances, even to know, even in a rough way, what's going on. And

therefore, people who were free to write and think about this in a strategic way didn't know enough to do it.

And so here we have a whole war machine built around this, and we haven't begun to think at all about ways to control its use. And then, you know, as some things are now known, the US and China have started talking about-- I mean, it's still very primitive. It's like talking about ways to set up a forum which might discuss how to set up another forum to discuss the issues that need to be discussed. And that's just the US and China. There's nothing that's been going on in that way with Russia, with Iran, Syria, North Korea, France, Israel. I'm not saying it can't be done. But we are at a very, very primitive stage.

JOE MCGONEGAL: We're a Dis-United Nations right now.

FRED KAPLAN: There's not even a committee in the UN, as far as I know, that's even set up to talk about it.

JOE MCGONEGAL: Tell me what else you're reading right now.

FRED KAPLAN: What am I reading now? I just finished Laura Secor's excellent book called *Children of Paradise-- The Struggle for the Soul of Iran.* I'm halfway through the first volume of Sidney Blumenthal's biography of Abraham Lincoln, which is really excellent.

JOE MCGONEGAL: Fred Kaplan's new book is *Dark Territory-- The Secret History of Cyber War,* published this spring by Simon & Schuster Press and available at your favorite local bookstore. Fred Kaplan, thanks for joining me.

FRED KAPLAN: OK, thank you.

[SLICE OF MIT THEME MUSIC]